ActualTech Media

solarwinds

Modern Backup, Under the Hood

Trevor Pott & James Green

CONTENTS

INTRODUCTION

If you are reading this, you're taking time out from a busy schedule looking for reasons to pick one data protection solution—in this case, SolarWinds backup—over another. Your time is valuable, and SolarWinds let an actual SysAdmin write this paper, so let's do that thing they normally never let us do: dispense with the buzzwords and just talk shop.

If done right, data protection is unsexy. But that's not a bad thing. You don't want data protection to become exciting; such events have an unfortunate tendency to lead to negative headlines. Unfortunately, the mundane rarely holds one's attention for long, meaning that automation plays an important role in staying out of those headlines.

SolarWinds understands the importance of automating the boring parts of data protection, which is why SolarWinds Backup is so easy to use.

Why SolarWinds Backup

Addressing the elephant in the room, SolarWinds Backup is marketed as cloud-first backup. The goal of this product is to get you to send your data offsite. This is both good and bad.

The 3-2-1 backup paradigm that the majority of the IT industry has accepted as canonical states that organizations should keep three copies of their data, on two different mediums, with at least one copy offsite. There's some wiggle room in the "two different mediums" bit (if it's on disk both in production and at the data protection site, is that one medium, or two?) but the offsite part of this is a must-have.

If your data doesn't exist in at least two places, then it doesn't exist.

Sending your data offsite is an act of trust. You're trusting the organization that operates the data protection location to not lose or misuse your data, which includes not giving your data away to someone else.

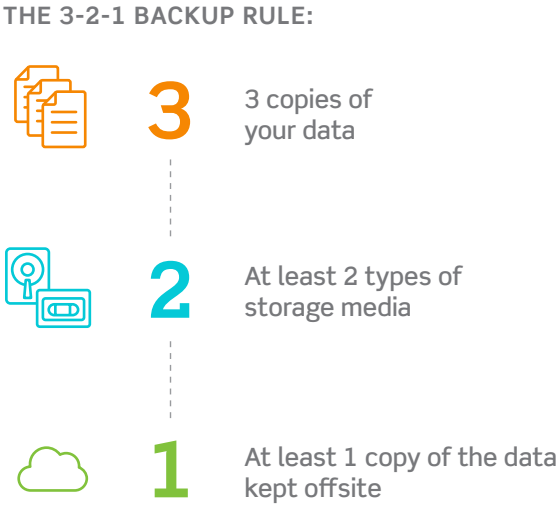
Unlike many vendors who simply wave away privacy and data sovereignty concerns as the irrelevant occupation of a paranoid fringe, SolarWinds understands that trust is hard. SolarWinds Backup has been designed with the fragility of trust in mind.

Secure, Compliant Cloud Storage

SolarWinds doesn't want to be able to pry your backups open. To this end, they've designed SolarWinds Backup to use AES 256-bit encryption both at rest and in transit.

The 256-bit encryption has 1.1 $x10^{77}$ possible combinations. Even with the most advanced known techniques—ones specific to AES, and not restricted to optimal theories about key space size—it would take longer than the Earth will be habitable to crack AES 128, and longer than the universe itself has existed to crack AES 256. For this reason, AES-256-bit is considered to meet the standards required for military use.

Of course, encryption algorithms alone don't determine whether an encrypted backup is secure. What really matters is how the encryption keys are handled.



SolarWinds Backup supports both private key and centralized key management solutions, both of which are entirely under the customer's control.

With private key management, the organization handles their own key management. For those organizations looking for more ease of use, SolarWinds Backup also provides integrated secure, centralized key management.

Encryption in-flight is provided via TLS 1.2 tunnels, and the data is physically stored in ISO 27001-certified data centers. These data centers comply with the SSAE 18 auditing standard, and meet Service Organization Control 1 Type 2 requirements covering the data center's internal control over financial reporting.

And finally, since the data traveling to/from the cloud in daily backups is only the compressed and deduplicated changed bytes, these fragments would be unlikely to mean anything to anyone who could get past all these hurdles.

Compliance

These compliance standards are generally considered to meet the requirements for storing sensitive Personally Identifiable Information (PII). SolarWinds Backup data centers are certified to hold data regulated under the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPPA) and the Payment Card Industry Data Security Standard (PCIDSS).

That means that much effort has been put into everything from physical security design to business processes and auditing. The end result is that data center operators have tight controls over who can access the data stored in these data centers, and that every access is logged and audited.

There are 15 SolarWinds data centers to choose from for data protection. While data center selection in and of itself cannot make an organization compliant with various regulatory regimes, choosing the wrong data center—or data protection solution—can make achieving compliance difficult, if not impossible.

> An organization's data belongs to that organization, and SolarWinds is committed to ensuring that it stays that way.

Some regulatory standards, such as the European Union's General Data Protection Regulation (GDPR), require far more effort to be put in than simply checking off compliance boxes. Care must be given not only to where the data is stored, but also to who can access that data, when, and under what circumstances.

Privacy and data sovereignty concerns may require that organizations store their backup data not only in data centers meeting a high standard of security compliance, but also that the data be physically stored within specific jurisdictions. SolarWinds's global data center footprint includes data centers in the United States, Canada, the United Kingdom, Netherlands, Germany, Italy, Switzerland, Norway, France, Australia, and South Africa.

SolarWinds is committed to building the SolarWinds Backup solution globally; that includes not only the ongoing expansion of physical data center locations, but a continual review of security, privacy, and data sovereignty concerns around the world.

SolarWinds doesn't want to be just another backup vendor selling their solution based on checkbox compliance. The goal is to earn a reputation for being the one vendor that understands that not every country, organization, or backup administrator has the same view of regulatory compliance. An organization's data belongs to that organization, and SolarWinds is committed to ensuring that it stays that way.

Deployment and Data Efficiency

The selling points for SolarWinds Backup don't begin and end with a focus on privacy, security, and data sovereignty, however. While these are critical considerations for any cloud-based backup solution, none of that is relevant if organizations can't get the data from point A to point B.

As with any backup solution, SolarWinds Backup consists of three components: the bit that does the backups, the bit that manages the backups, and the place the backups get stored. With the storage portion thoroughly explored, the other two pieces to the puzzle deserve some attention.

SolarWinds' control plane is cloud-based. This means that management tools are not required. Backup administrators simply register, login, and begin. The management console is an HTML 5-delivered interface.

Backups are performed by backup agents. These agents are installed on physical or virtual servers, as well as endpoint devices. There are several deployment options available, ranging from a standard interactive install wizard to packages suited for software deployment tools or command-line-based deployments.

SolarWinds Backup makes use of a number of data efficiency technologies to reduce the burden on an organization's internet connectivity. SolarWinds Backup uses compression in addition to advanced technologies such as byte-level deduplication to help reduce the size of the data to be transmitted, though this is only the beginning of the work that goes into optimizing backup data.

SolarWinds Backup's TrueDelta combines the byte-level deduplication with a Changed Block Tracking (CBT)-like technology to ensure that only data changes since the last successful backup are backed up. It performs an initial backup that contains a full copy of the data to be protected, and from that point forward, backups are incremental.

For upload to private cloud storage, deltas are packed into Cabinets, which means less outbound connections, lower network latency, and faster transmission of the total payload. The Cabinet size is optimized for transmission over IP networks, as well as for efficiently laying down on disk once it lands.

The result of this data efficiency is an order of magnitude reduction in data transmission. Consider a customer with 4,301,194 files occupying 8,190GiB of space. This customer's average daily data change is 0.70%, or 409.5GiB per day. Of this, only 4.03GiB of data was sent to the cloud per day after deduplication.

Details

Unlike Cloud Storage Gateway (CSG)-based backup solutions, data is not necessarily copied to a cloud storage gateway before being uploaded to the cloud. This approach has some real-world consequences of which backup administrators should be aware.

In a CSG-based cloud backup, deduplication and compression is typically performed by the CSG. This allows the CSG to achieve higher deduplication ratios because it can store the complete manifest of all blocks. The CSG also uses its CPU power to perform the deduplication and compression, resulting in minimal overhead to individual workloads.

The price to be paid for CSG efficiencies, however, is that CSGs are themselves both a significant capital expense and an ongoing operational and management expense. In addition, CSGs buffer data that is sent to the cloud and unspool it over time. This means that backup arrival at the data protection destination can be delayed for several hours when compared to a direct backup approach, which lengthens Recovery Point Objectives (RPOs).

SolarWinds Backup agents communicate directly with the data protection destination. This distributed approach scales as environments grow, as opposed to a local appliance that is often quickly underpowered or obsolete. This approach shortens RPOs, but does so at the expense of imposing the data efficiency CPU overhead on the individual workloads. Fortunately, in practice, this overhead has proven to be quite small. At most, SolarWinds uses a single CPU core or hyper-threaded core for processing the backup and for bi-directional synchronization of local and cloud storage.

The Third Copy

The "3" in the 3-2-1 backup paradigm is about keeping three copies of your data. Thus far, only two copies of the data have been discussed: the production copy and the data protection destination (the cloud) copy. In an ideal scenario, a third copy of the data exists in the form of an on-premises backup vault.

The purpose of an on-premises backup vault is to reduce the Restore Time Objective (RTO). The amount of time it takes to pull down an entire workload from the cloud depends on the speed of one's internet connection. For some workloads, this may be an unacceptably long delay (excepting under disaster circumstances.)

> "You get paid for backup performance, but you keep your job with recovery."
>
> – THOMAS LaROCK, SOLARWINDS

For this reason, SolarWinds Backup is able to use a LocalSpeedVault. LocalSpeedVaults can be a directory on a local disk, a removable disk, or a server share or NAS device located on the local network. The LocalSpeedVault has two advantages:

- It enables more rapid restores than a cloud-only backup
- It offers a backup destination for workloads during brief internet connectivity outages

While a useful feature, LocalSpeedVault is not ideal for all workloads. Backing up to an on-premises storage location requires storage forecasting, provisioning, and expansion of storage over time. This is exactly the sort of storage management overhead that makes cloud-based backups so attractive.

Using LocalSpeedVaults for all workloads would reduce the cost savings of direct-to-cloud backups, but this is offset by the advantages of faster RTO and data redundancy.

The ability to use existing dumb disk hardware is more attractive to many than a proprietary appliance.

But costs can really drop due to the fact that SolarWinds also includes the cost of cloud storage in that base price. This means that the cost of protecting workloads that don't require the use of LocalSpeedVaults can be dramatically lower than the cost of protecting those same workloads using a data protection solution that requires a local storage vault or CSG to operate.

Acing Restores

While all the details of how data is backed up and stored are important, restores are what really matter. If you can't restore your data, then it doesn't exist. SolarWinds Head Geek Thomas LaRock puts it succinctly: "You get paid for backup performance, but you keep your job with recovery."

SolarWinds is aware of this, and significant effort has been put into not only making sure that restores are reliable, but also to ensure that they're performant and simple. On the performance side, the optional LocalSpeedVault acts as an on-premises backup cache to accelerate restore operations. In addition, bi-directional byte-level data deduplication and WAN optimization mean that the same data is never sent over the wire twice.

Block-level restore granularity means only changed blocks are restored. While this provides no advantage in situations where an entire workload must be restored to a fresh environment, it means that rolling back workloads to a previous version only requires downloading those blocks that are different between the two versions.

To ensure reliability, SolarWinds Backup includes a recovery testing function to ensure that backups are good. This avoids the Schrödinger's backup problem, where administrators don't know if a backup is good until they try to restore it. SolarWinds Backup also offers automated recovery with email confirmation and screenshots for both VMware® and Hyper-V® environments, further freeing backup administrator time.

SolarWinds is also aware that the majority of restores do not occur at workload scale, but instead are about recovering a single file, or collection of related files. This is can be due to ransomware, accidental deletion, or simply having gone in the wrong direction on something and wanting to go back to before everything went sideways.

SolarWinds Backup offers a feature called Virtual Drive which makes file-level restores simple and convenient. Virtual Drive can offer local file recovery. Users can also mount a drive-in Windows® Explorer® and view historic backup session as a browsable file system, similar to Apple's Time Machine.

Myriad Restore Options

Disaster recovery is a concern for many backup administrators because the environment available for restoring workloads may not be identical to the one from which those workloads originated. To address these concerns, in addition to the previously discussed restoration methods, SolarWinds Backup offers advanced restore options that provide significant disaster recovery flexibility.

Backup administrators can use the Recovery Console to automatically create and update standby images (or remote recovery copies) of selected data on a schedule. This helps easily create a warm disaster recovery setup for planned failovers.

SolarWinds Backup also offers Continuous Restore. This does exactly what it sounds like it does: backups sent to the SolarWinds cloud are also sent to a disaster recovery site, and that site is constantly ready to take over at a moment's notice from the primary site.

SolarWinds Backup can restore workloads to any number of target destinations. Cloud recovery targets include infrastructures controlled by the organization; Microsoft® Azure®; and hosted VMware vSphere® or Microsoft Hyper-V-based environments located at service providers.

Finally, both physical and virtual workloads can be restored to dissimilar virtual hardware, while bare-metal recovery (via bootable image) simplifies and reduces recovery time for Windows servers.

SolarWinds Backup keeps your business available economically and with unrivaled ease of use. From sign-up to backing up, organizations can start protecting their data in less than five minutes. Try SolarWinds Backup today.