NOVASTOR

WHITEPAPER

How to Sell A New Backup Solution to Your Boss

Introduction

It's time for a new backup solution, and while you know it, your department or division head may not be aware of the technical issues at hand. They may require some convincing. The fact is that backup is something everyone knows is necessary but expects to work silently in the background. A technology which is nearly invisible can be challenging for executives to dedicate budget resources towards, but every minute that critical data sits inadequately protected may actually be costing your organization money. Upgrading and replacing a backup solution is something that is often delayed until a disaster strikes or data loss occurs – at which point the damage is already done.

Get ahead of the game. You've identified that a new backup solution is necessary and done some research. Now let's put ourselves in your bosses' shoes and consider the pressures they will endure with adopting a new technology. Let's anticipate some of the questions they will have for you and prepare to demonstrate what your organization needs in order to properly secure critical data.

Influential Factors

- Initial Cost
- Time to Implement
- Time to Backup / Restore
- Compliance
- Scalability
- Support
- State of Denial

Factor: Initial Cost

Businesses, especially small ones, expend as little budget as possible for reliable backup, and therefore, they need a vendor that offers flexible licensing models. A perpetual license model provides full software ownership, while a subscription license option ensures that software is always current and that support maintenance is always valid. A backup vendor should also offer competitive upgrade pricing, making it worth the move to a new solution. If your boss has a "if it ain't broke, don't fix it" mentality, then you must be able to demonstrate why the existing system is either too costly or how a new backup system offers financial benefit.

NovaStor recommends that you bring to the table evidence that this investment in security is profitable. How?

Cost of Existing Backup Solution

If your existing solution is reliable but cost-prohibitive, this document should include:

- Software and hardware costs, including license renewals, anticipated upgrades, etc.
- Cost of ongoing technical support/maintenance (or expected pay per incident)
- Cost in man-hours to administer backups for each machine (including hardware)
- Cost to maintain backup storage and media

Cost of Downtime (Per Hour x Expected Recovery Time)

Even with huge differences in the way that businesses operate, Gartner estimates the average cost of downtime at $5,600/minute. How many minutes will it take your solution to restore?

Gartner estimates the average cost of downtime at $5,600/minute

If your existing solution has questionable reliability, this document should include:

- Expected business revenue over an average 40-hour work week (existing and new sales)
- Expected fixed costs (wages, utilities, etc.) over a 40-hour work week
- Expected amount of time to recover from a mild/medium/severe disaster
- The estimated cost of a backup recovery scenario between lost revenue, fixed costs, and lost productivity

Return on Investment

Your new, reliable, and efficient solution is going to save your company money as well as keep critical data secure, but you must be able to present how long it will take to recover an investment in new technology. Therefore, your document should include:

- How many daily internal administrative hours are saved following implementation
- How are external licensing, maintenance and support costs reduced
- Factoring in a single downtime incident (how much is saved in recovery time)
- How are infrastructure costs reduced (power, machines, data storage, cooling, etc.)
- Projected increase in reliability and productivity

Factor: Time to Implement

Integrating a new solution can take time. Time is the asset that small businesses have all too little of, so the fear that "This is not a good time" to make the move to something new is a legitimate one, but the vetting and testing of a new backup solution can be accomplished in a controlled environment without disrupting day-to-day operations. A transition can then be phased-in through steps so as to not disrupt operations. If your existing backup solution is costing you time on a daily basis, then postponing a change only results in further loss. A clear migration plan allows those outside of the IT department to visualize the change and move forward with a level of confidence.

Download NovaStor's Tips for Migrating Backup Solutions

Create A Migration Plan

- Download NovaStor's Tips for Migrating Backup Solutions
- Analyze where data lives, and how it will be cleaned up and prepared for migration
- Determine what hardware and storage changes must take place
- Create a visual timeline that details which databases and applications will be backed up during which phase of the migration to a new solution

- Plan to decommission the old solution in sections, with a verification phase
- Consider how migration could affect possible downtime
- Create a fall back plan for each migration phase, should an unexpected problem occur
- Plan to maintain dual solutions, if possible, for a length of time

When presenting your Migration Plan, it is best to offer options and maintain objectivity, giving decision-makers the data to make informed decisions for the business. Another item to consider is time spent training and adapting to a new solution. Fortunately, many backup solutions like NovaStor's DataCenter, offer a simple installation with minimal hardware requirements. This makes it easy to get familiar with a new backup process at your own pace. Here's how:

- Request a walk-through from the vendor
- Request a fully functional demo solution for your environment
- Install and test the new solution on an available physical or virtual machine
- Request a proof of concept from your vendor that is specific to your environment
- Attempt to duplicate regular backup jobs using the new technology
- Prepare to demonstrate the new test environment for decision-makers

Factor: Time to Backup / Restore

Your backup window is the available slot of time in which backup jobs can initiate and back up critical data. And the amount of time that it takes to recover from a data loss incident and get back to business, can never be small enough. These two intervals are often what businesses hope to improve most when it comes to upgrading backup solutions. How much will your backup and restore times improve? It's a complicated question that depends on size of data set and connection speeds (among other things). But if you opt to use NovaStor DataCenter, you can reassure your boss that the new solution will be backing data up locally for fast restores, as well as offsite and/or in the cloud for redundancy.

If your existing backup solution is not performing acceptably, it must be demonstrated how the business is being placed at risk.

Backup Time

Is your existing solution failing to meet the backup window? Document these incidents, such as:

- Backups extending into production hours affecting network performance
- Inability to start new backups because old backups have not completed
- Intentionally disregarding data sets so that backups can complete
- Sacrificing other maintenance tasks to offer more time for backups

Restore Time

Performing a backup restore test on at least a quarterly basis should be part of every backup administrator's agenda, but there is a nearly fool-proof method of determining how long it would take to restore in the event of a data loss emergency:

There are many methods for testing backup restorability. Here are a few examples:

1. Import a full backup and restore a few individual files
2. Import a full backup on a different system, restore individual files
3. Restore a virtual machine, mount and log in to verify usability
4. Mount System Image backup and restore individual files
5. Restore System Image entirely to alternate hard drive
6. Restore an Application Database and check for consistency

By following your disaster recovery process and simulating a real-life data loss situation, you can better estimate and document how much downtime would be required to get your organization back up to full performance, and whether this is acceptable. How much might a 5%, 10%, or 20% improvement in recovery speeds affect company profits/losses?

Factor: Compliance

Is your current backup solution providing compliance with industry regulations like HIPAA, FERPA, PCI-DSS, SOX, GDPR, etc.? A properly configured backup solution keeps private information securely stored and encrypted, an important element of these regulations. If you are out of compliance, your organization may be in a precarious position, not only at risk of a serious security breach, but also at risk of huge fines should a breach occur. These types of fines are generally amplified by negligence, meaning that a best effort should always be made by a business to protect customer information.

Examples of Compliance

- HIPAA
- FERPA
- PCI-DSS
- SOX
- GDPR

If you'd like to offer your boss some examples of businesses who have been hit with recent fines, you'll have no shortage of examples to choose from:

HIPAA – University of Texas MD Anderson Cancer Center in Houston, $4.3 million in civil penalties for HIPAA violations related to encryption - 2018

DC Data Breach Laws – Uber settles with attorney generals of all 50 states and the District of Columbia, $148 million, 2018

GDPR – Facebook could face up to $1.63 billion in the EU following a data breach that hit 50 million users

Beyond opening yourself up to legal fines, the liability could also open up the opportunity for lawsuits. NovaStor recommends following a basic set of backup guidelines which are common to many industry-specific security regulations. Your boss should understand that a backup solution must be able to accomplish the following:

- Data must be backed up frequently
- You must be able to fully "restore" any lost data
- You must also be able to demonstrate that you have tested the restorability of backups frequently to ensure data recoverability
- You need to have a copy of your critical data in a separate location
- Data must be encrypted to prevent unauthorized access
- You must prepare written procedures related to your backup and recovery plan. Showing your intent and taking the time to document the protection of your data could protect you from penalties.
- Someone should be dedicated as the officer in charge of data security training
- Applications, operating systems, and drivers should be kept current

Those who follow these basic tenets will find themselves in a much better position to avoid significant disaster and demonstrate that they did everything within their power. There are numerous stories of organizations that were saved from unnecessary fines by providing a best effort when it came to data protection. Bring one of these positive success stories from a similar business along with you to the next meeting with your supervisor to balance out any uneasiness.

Factor: Scalability

As a business grows, so does its data. One reason that you may be considering a new backup solution, is that your existing backup lacks the ability to scale with the growth of your organization. A solution that is failing to scale will hurt an organization both in terms of performance and cost effectiveness. Let's take look at these individually.

Scalable Technology

On one side of the coin, you should be able to demonstrate the technology features in a superior solution that will lead to improved backup performance.

- Distributed Architecture – Distribute backup clients across the entire enterprise, including remote locations, as your command server instruct the clients when and where data is to be sent. Designed so that backup devices take the path of least resistance, maximizing performance and speed by streaming data directly to storage destinations.
- Redundant Metadata - A backup solution should never rely exclusively on the integrity of a central database to restore. In the event all servers are lost, backup media should still be quickly restorable without lengthy import.
- High Performance Data Movers - Minimizing system load while maintaining the highest data throughput: Optimized compression distributes the processing load to both the client and storage medium.
- Multistreaming - Send multiple streams of data, from a single client, simultaneously and/or multiple streams of data from multiple clients simultaneously to a single backup server.
- Multiplexing - Taking multiple data streams and streaming them to a storage medium, like a tape drive, in order to utilize the full bandwidth of the device.

Does your existing backup solution offer these features to quickly scale? If not, these are key technologies that can be brought to the attention of decision makers.

If your business has plans to add new servers, workstations, virtual environments or office locations, it must be determined how the backup solution can adapt to quickly meet the needs of expansion. How quickly can backup clients be deployed and new data secured? What about critical data stored on the roaming laptops of executives? Can physical and virtual machines be managed through the same solution? If excessive time is required to accomplish these tasks through the existing solution it must be documented in detail.

> A solution that is failing to scale will hurt an organization both in terms of performance and cost effectiveness.

Scalable Licensing

Beyond the technical ability to smoothly scale and support a business's needs, it must also be cost-effective to do so. When it comes time for a business to add support for additional servers, applications and hypervisors – many popular solutions require the purchase of additional agents and plugins. This tendency by backup vendors to charge "per feature" can blindside administrators who have fixed IT budgets and yet find themselves in an expansion phase.

You should be able to demonstrate to financial executives that a new backup solution is ready to support business growth though a clear, predictable cost model. Look for solutions that offer software licensing cost structures like:

- All-inclusive features (no additional agents, or plugins required)
- Included support for multiple operating systems
- Included installation, training, and setup assistance
- Competitive upgrade pricing
- Ability to bundle multiple technologies (software and storage, etc.)

- Predictable recurring cost guarantees
- Site licensing options

It can be highly beneficial to build a sample growth model and a forecasted cost-comparison between your existing solution and potential replacement backup solutions.

Factor: Support

Many organizations feel treated like royalty – before they make the purchase. However, once the deal has closed, they may find that they are no longer at the top of their backup vendor's priority list. They may even be sent to long distance call-centers for support and be forced to prove that they've already attempted the obvious. For a business who has set aside a large piece of their IT budget specifically for backup support, this is unacceptable.

As you prepare your arguments for purchasing a new backup solution, have a clearly documented history of your support calls and how they were addressed. Some measurable factors include:

As you prepare your arguments for purchasing a new backup solution, have a clearly documented history of your support calls and how they were addressed.

- Amount of time it took to receive each initial response from your existing vendor
- Amount of time between support request and support responses from your existing vendor
- The ratio of issues resolved via the first contact
- Average amount of time it took for an issue to be completely resolved

Moving to a backup solution that is support-centric can offer several relationship upgrades.

- Setup Assistance Included VS. Additional Cost
- Personalized Training VS. Self-Training
- Dedicated Employee Representative VS. Outsourced Call Center
- Backup Engineers VS. General IT Support Staff
- Access to Management Team VS. Dead Ends
- Recurring Health Checks VS. Going It Alone

A new backup vendor should also be able to offer customer references of similar organizations that you can independently contact and get their honest opinions regarding technical support.

SUPPORT TEST: Want to get creative? Reach out to a vendor's support team prior to making a purchase and get a feel for how they respond to your questions, issues, and requests during the trial phase. If they aren't helping you now, how can you be sure they will be there after purchase?

Bonus Factor: In a State of Denial

Let's face it, some bosses may have never seen serious data loss occur and therefore doubt how at-risk the business might be. They may be suffering from a mentality that "we're not big enough" to be the target of an attack.

If you find yourself in a situation like this, it may be the perfect time to simulate a fake phishing or ransomware email for the purpose of gathering statistics. Imagine an employee opening a personal email while on a break. They click on a malicious link or file and it launches a script that brings ransomware into the business. You would be wise to get your boss' buy-in on any sort of test and you may even choose to warn employees well in advance that a company test like this may occur. Here are some examples:

- Impersonating an employee with a requested unauthorized click-action
- Impersonating a file sharing service (Dropbox, etc.) asking to click an unauthorized link
- An email sent to accounts receivable refusing to pay an attached bill (open a file)
- An email from a partner asking to review the attached contract (open a file)

Depending on the procedures and training within your organization for the use of private company information, a test like this can yield surprising results. If click through rates are measured, a report is easily generated detailing internal weakness. These types of attacks are common and are increasing in methods of sophistication, coordination, and impersonation.

If you are ready to purchase backup software,
please visit our website for pricing and other details at www.NovaStor.com