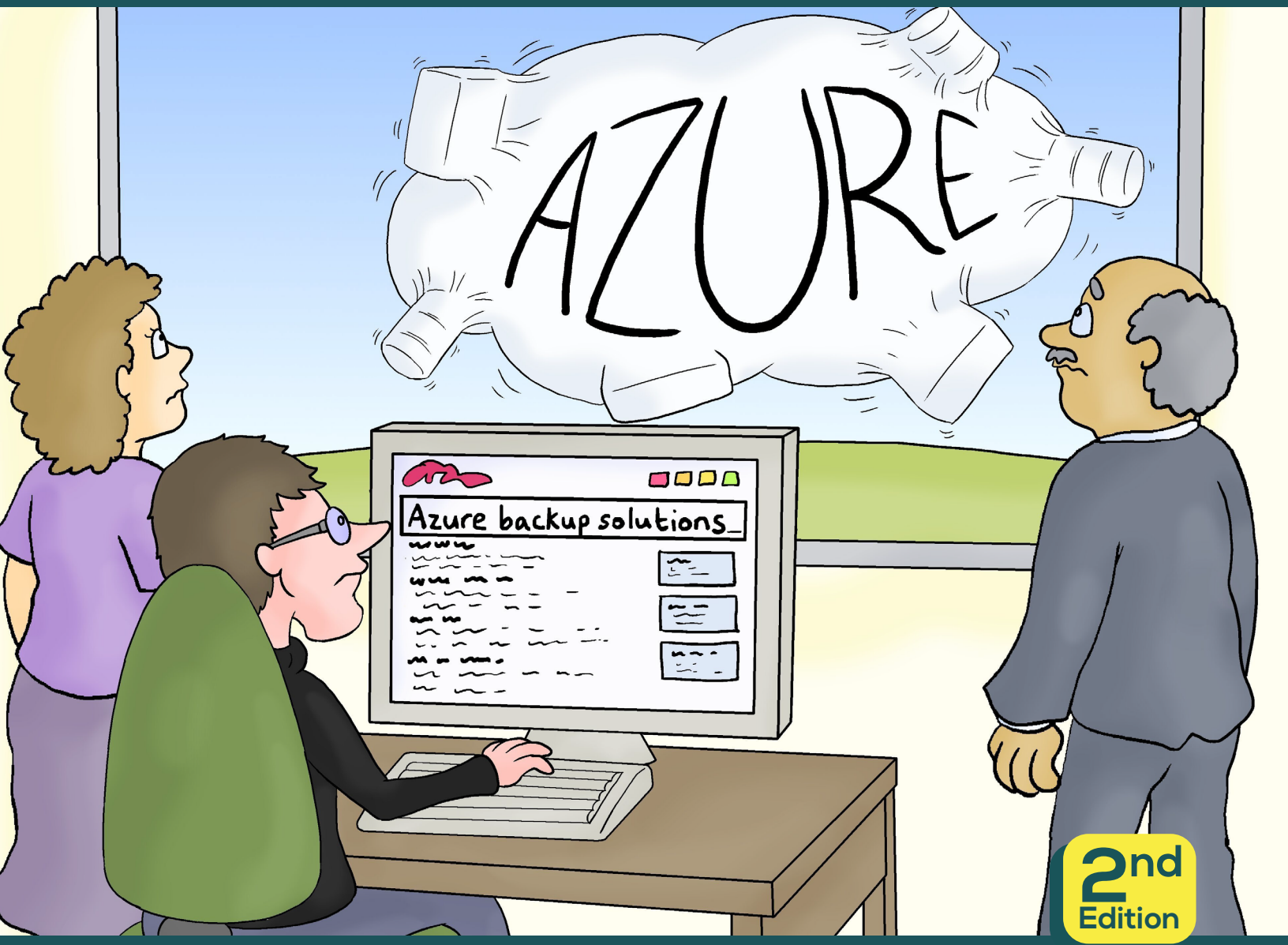
ConversationalGeek®

Azure Backup Solution
Buyer's Guide



Sponsored by veeam

Azure Backup Solution Buyer's Guide

Published by Conversational Geek® Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Choosing the Right Azure Backup Solution

The Azure cloud offers built-in mechanisms that can help an organization to back up its data. As an organization grows however, it may find that these native options quickly become inadequate, often causing ballooning costs, or lock-in to the Azure platform. . Fortunately, there are numerous third-party backup solutions available in the Azure Marketplace.

You're reading this Buyer's Guide because you know that your current approach to Azure backups just isn't working anymore, and you need something better. The question then becomes, how do you pick the right solution that will meet your own unique needs. In this buyer's guide, I'll cover the critical (and nice to have) capabilities that are found in modern Azure backup solutions. I'll also provide you with some worksheets that you can use to figure out which of the available solutions are right for your organization.

- Brien Posey

Table of Contents

How to Use This Guide

How to Use This Buyer's Guide

Conversational Geek Buyer's Guides help you assess and choose the right solution for your organization. *We do this by breaking the guide into two parts.*

Buying Criteria

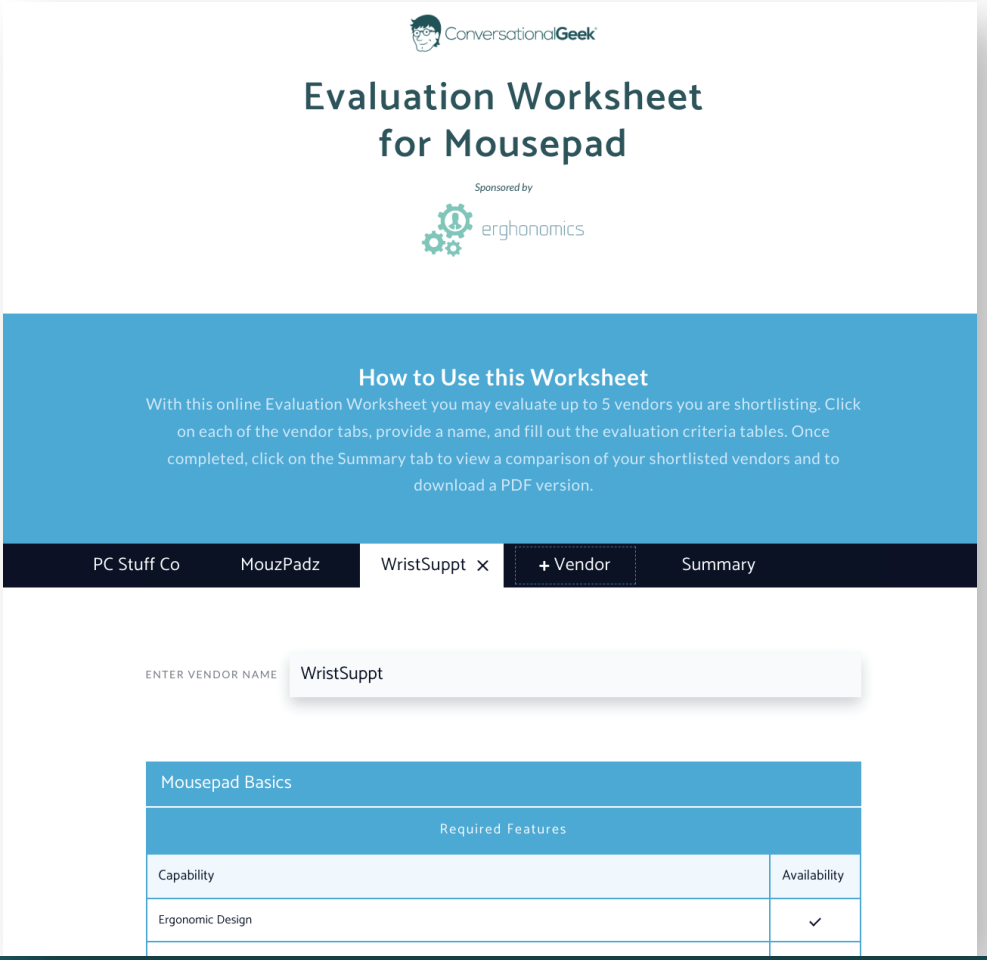
We first provide you with a number of important buying criteria to consider here in this PDF. Each criteria section focuses on a particular set of features and capabilities available by solutions today. Those capabilities are then broken down into two distinct categories:

- **Required:** The capabilities listed in this criteria category are those that are fundamental for purchase consideration. Any solution you consider on your shortlist should have the capabilities listed at a minimum.
- **Optional:** The capabilities listed in this criteria category are features that will enhance your use of the solution but aren't part of the core required capabilities. An optional capability might be considered innovative in nature or simply be of value but only to organizations with specific needs.

Start by reading the *Buying Criteria Detail* portion of the Buyer's Guide, taking note of which capabilities are important to you, regardless of whether they are listed as *Required* or *Optional*.

Evaluation Worksheets

We then provide you with a URL that points to an online Evaluation Worksheet designed to let you evaluate each solution you are considering – and determine a winner.



Buying Criteria Detail

Backup

Recovery

Storage

Security and Compliance

Management

Backup

The most basic requirement for any Azure backup solution is its ability to back up an organization's data. This criteria section focuses on the backup product's ability to protect your data and to scale as the data footprint becomes larger.

Required Features

- **The Ability to Protect All of Your Azure Data:** The Azure Cloud offers dozens of services, and a good cloud backup solution needs to be able to natively protect the services that you use. At a bare minimum a good Azure backup solution should offer protection for Azure Files, Azure VMs, and Azure SQL, but can also include Managed Disks and Azure SQL Managed Instances.
- **Ability to Choose Backup Appliance Sizes:** The Azure backup solutions that are available in the Azure marketplace are generally installed as virtual appliances. It is important for an organization to be able to choose the size of the underlying virtual machine that is being used by the virtual appliance. Otherwise, smaller organizations may end up overpaying because the virtual machine is larger than what is needed to back up their organization. Conversely, a large organization might find that a virtual appliance is too small to meet their needs. Being able to select the virtual appliance size is critical to rightsizing Azure backup operations.
- **Data Compression:** Data compression is a must have for any Azure backup solution. Microsoft bills Azure subscribers based on the resources that they consume. Compression can help to reduce both bandwidth and storage consumption. Additionally, compression can expedite the process of sending backup data to another region.
- **Policy Based Selection of Workloads Protected:** Virtual machines and other workload types tend to be highly dynamic, with new machines being created all the time. You shouldn't have to manually modify a backup job just because someone creates a new Azure VM. Instead, a good Azure backup solution should allow policy-based workload selection (based on tags or other mechanisms) so that newly created VMs and other workloads are automatically backed up, with deleted workloads automatically excluded from backup jobs without producing an error.
- **Application Consistent Backups:** Backed-up data needs to be transactionally consistent to ensure that a given application will boot up post-restore. To attain this, applications need to flash all transactions to disk, leaving no unfinished transactions when taking VM snapshots.
- **Backup Verification:** Snapshot backups should be tested for durability to ensure recovery is not only possible but will achieve a predictable result.

It All Starts with Backups

Backup is the most basic, yet critical function for any Azure backup tool. As such, it is important to make sure that an Azure backup product is able to back up data in a way that will meet your organization's requirements both with regard to RPO and RTO, and with regard to the types of data that it can protect.

- **Backups Sent Directly to Hot, Cold, or Archived Azure Blob Storage:** Any backup solution that is designed specifically for Azure needs to be able to recognize the various tiers of Azure Blob storage and to be able to use any of these tiers as a backup target. Backup jobs can have differing storage needs and so it is important for a backup application to offer the flexibility to store backups on the tier that makes the most sense for that job.
- **Data Retention Policies:** An Azure Backup solution should allow admins to create policies dictating the length of time for which backups are retained. Additionally, there should be a policy setting that enables aging backups to be automatically moved to lower cost Azure Blob storage.
- **Data Portability:** As organizational policies toward cloud adoption evolve, it's important to consider whether or not data can be moved out of the Azure cloud entirely. Snapshots themselves are often locked to the storage type, but creating a backup may unlock a much-needed insurance option down the road.

Optional Features

- **Hybrid Backup Support:** Some solutions may offer an ability to backup both your on-premises and Azure-based VMs and data to one solution, allowing organizations to potentially protect all of their operational environment. These features help to standardize your backup strategy, ensuring no workload is left behind in the shuffle of multiple point products.
- **Create Multiple Backup Appliances:** An Azure backup product should not limit you to using just one virtual backup appliance. Being able to create and use multiple virtual backup appliances allows for backup scalability since the appliances can work in parallel, each backing up a subset of the data. Additionally, having the ability to create multiple backup appliances can sometimes help to reduce costs. This is especially true when an organization can map smaller virtual backup appliances to smaller data sets and larger virtual backup appliances to large data sets. Mix matching virtual backup appliance sizes helps to ensure that each appliance is perfectly matched to the workload that it is protecting.
- **Running as a Native Azure Virtual Appliance:** Modern Azure backup solutions should natively deploy as an Azure virtual appliance. You shouldn't have to manually create an Azure VM and then install backup software on to it. Such installation requirements typically indicate that the backup software was originally intended for on premises use and is not truly cloud native.
- **Multi-Tenancy Support:** It is becoming increasingly common for organizations to have multiple Azure subscriptions. As such, it is helpful if a backup solution can protect resources that are running in other tenants.

- **Cross Cloud Backup Support:** For some organizations, having backups residing in the same environment as the backup sources may not be enough to ensure recoverability. Azure backup solutions may employ automatic replication of data to other Azure accounts, regions, and edge locations, as well as other clouds, including the backup solution vendor's own cloud.

Recovery

For a backup product to be of any value at all there must be a way to recover the backups that have been created. This criteria section focuses on what is involved in restoring Azure data.

Required Features

- **Granular Recovery of VMs:** Although recovery operations often center around VMs, not every restoration justifies restoring the entire virtual machine. A good Azure backup product should allow you to choose exactly the data that you want to recover. This means allowing for the restoration of the entire virtual machine, a single volume, or even individual files.
- **File Level Recovery:** It is necessary to be able to restore individual files from a VM. The backup solution should allow you to browse a VM's file structure and then restore files either to the original or to an alternate location.
- **Cross Cloud Recovery Support:** In today's world, multi-cloud has become the norm. Although an organization might have data residing in Azure, it doesn't mean that that will be the data's location forever. As such, it is important for an Azure backup product to offer a way of restoring data to other clouds such as those operated by Amazon or Google.

Optional Features

- **Use of Orchestration Automation:** Many backup vendors also offer an ability to create automated recovery scenarios that orchestrate the recovery steps necessary to put all the needed data sets, and workloads back into place in the correct order. It makes sense that orchestration features should support recovery into Azure.
- **Power on VM After Recovery:** Virtual machine recovery operations can sometimes be time-consuming, and a backup operator might not always know the very instant that a recovery operation has completed. Having an option to automatically power up newly restored virtual machines can help to bring workloads online more quickly because it eliminates the need for the backup operator to recognize that the restore operation has finished.

Recovery's Value is in the Details

A backup is no good if you cannot restore it. While any Azure backup product should presumably allow you to create a restorable backup, not all restore jobs are created equally. It's important to be able to restore exactly the data that you need without having to unnecessarily jump through hoops or restore everything and then extract the data that you need once the initial recovery job is complete.

- **Recognition of Credentials:** When restoring a backup, you can sometimes run into a situation in which credentials have changed since the time that the backup was created. Ideally, your backup software should be able to detect these types of credential mismatches and prompt you to enter new credentials rather than simply allowing a backup or recovery job to fail.
- **Restore a VM With Different Settings:** When recovering a virtual machine, Azure backup software should ideally allow you to restore the virtual machine with either the same or different settings. There are any number of reasons why such a feature might be useful. Restoring with different settings might for example, be used to assign a different IP address to a virtual machine or to place it on a different subnet. Similarly, there are situations in which virtual machines are restored for nonproduction years and it may not make sense to allocate the hardware resources that would be necessary for accommodating a production workload. Significant cost savings may be realized by restoring such a virtual machine to lower end hardware.

Storage

The Azure cloud provides several different storage classes, each of which has its own unique pricing model and intended use case. This criteria section focuses on a backup products ability to recognize the available storage classes and use them in the appropriate manner.

Required Features

- **Storage Tier Awareness:** The most basic storage related requirement for any Azure backup product is the ability to recognize the various storage classes and use them in an appropriate manner. A backup product should not for example, attempt to store archived data to hot storage or to store rapidly changing data to archive storage. An Azure backup product needs to consider both the performance and the cost before recommending a particular storage tier.
- **Ability to Use Multiple Storage Accounts:** Azure backups typically leverage a storage account. Even so, storage accounts are limited in the total amount of throughput that they can deliver. This means that if you direct multiple backup appliances toward a single storage account, it will likely deplete the available bandwidth and cause a massive bottleneck. As such, Azure backup products need to be able to support the use of multiple storage accounts, creating a logical air gap for much-needed resilience in the face of disaster or malicious attack.
- **Signature Support for Images & Links:** Allows recipients to easily connect with the sender through social media channels, delivering credibility and engagement on the part of prospects.

Where you Store Your Backups Matters

There isn't just one type of cloud storage. Microsoft and other cloud providers offer several different types of storage, each with their own unique cost and use case. It's important that any cloud backup solution be able to recognize the differences between these various classes of storage and use them appropriately.

- **Send On Behalf Signatures:** When utilizing Exchange's Send On Behalf functionality, clients can choose from one or more signatures assigned specifically for this scenario.

Security & Compliance

An organization's backups contain all of its most sensitive data, making security of paramount concern. This criteria section focuses on backup security features and those features that can help backup admins to adhere to regulatory requirements.

Required Features

- **Role Based Access Control:** While smaller organizations might designate one or two people to act as backup admins, larger organizations typically require a more granular delegation of privileges. A Role Based Access Control (RBAC) feature can make it so that an organization can assign a subset of permissions to specific users rather than giving all backup operators unrestricted access to everything. For example, an organization may wish to designate a particular user as a restore operator so that the user has the ability to restore backup jobs, but not the ability to create or modify backup jobs.
- **Logging:** Although it has long been a standard feature among backup products, logging is essential to knowing exactly what has been backed up and when. Logging takes on an additional level of importance for organizations in regulated industries, as it allows them to prove to auditors that data is being protected in the required manner.
- **Azure Key Vault Integration:** Many organizations use the Azure Key Vault to encrypt their Azure resources. An Azure backup solution should be able to use keys from the Azure Key Vault for backup encryption purposes.
- **Data Immutability:** Ransomware is easily one of the most pervasive threats to any organization's data. Having the ability to write backups to Azure's Immutable Storage for Azure Blob ensures that organizations will be able to recover their backups without concern that ransomware attack could modify or encrypt the backup target.

Optional Features

- **Multifactor Authentication:** Multifactor authentication (MFA) has long been a go to solution for preventing cybercriminals from accessing user's accounts through stolen credentials. Given the sensitivity of the data contained within an organization's backups it is important for a backup product to offer MFA support.

Backups Need to be Protected

Backups contain an organization's most sensitive information and must therefore be kept secure from accidental or malicious deletion, to the ever-evolving stylings of Ransomware and other cybersecurity attacks, securing backups requires a layered approach. Adding additional imperative, organizations and regulated industries must be able to prove to auditors that they are protecting data in an appropriate manner and retaining backups for the required duration.

Management

Azure backups are complex so a backup products management console should be designed in a way that helps alleviate some of this complexity. This criteria section focuses on some key features within an Azure Backup tool's management interface.

Required Features

- **Implementation Options:** Depending on the specific needs of your organization, the backup solution may need to be available in one or more models that include traditional self-managed software, cloud-based software as a service, or via a service partner as a fully managed service.
- **Management Dashboard:** Given that an organization can create a vast number of resources within its Azure subscription, it is extremely important for an Azure backup solution to include a dashboard that summarizes the state of the organization's backups. Such a dashboard should at a minimum list backups, archives, snapshots, and errors. Ideally, this dashboard will also provide information about storage consumption, cost, and performance. In addition to displaying a backup summary, the dashboard should allow admins to drill down into backup jobs to access additional details.
- **Snapshot Management:** Azure backups (with the notable exception of Azure SQL backups) are typically based on snapshots. If left unchecked, backup software can create an overwhelming number of snapshots. Similarly, the number of snapshots could also prove to be inadequate. As such, an Azure backup solution should be designed in a way that allows you to choose the number of snapshots to retain each day, as well as the length of time for which snapshots should be retained.

Optional Features

- **Prescriptive Guidance:** Azure backups can be complex and potentially expensive. As such, backup software should offer helpful advice that helps admins to avoid making common mistakes. If for example, an admin was to attempt to store long term archives on hot storage, the software might advise the admin that there is a more cost-effective option available (while still allowing the admin to make the decision rather than forcing best practices).

Managing Should Be Easy

A backup product is only as good as its management interface. Backup admins must be able to tell at a glance whether or not their backups are healthy, and they need features that will allow them to remediate problems and control costs.

- **Integration With On-Premises Backup Solutions:** Although cloud backups have increased in popularity in recent years, many organizations still have backup software that is running on premises. If an organization chooses an Azure backup product from the same vendor who makes the backup product that they are using on premises, then the two products should be able to communicate with one another in a way that simplifies backup management and provides enhanced options for data portability.
- **Configuration Backup:** Enterprise backups can be extremely complex, consisting of numerous jobs, schedules, targets, and other elements. That being the case, an Azure backup product needs to be able to back up its own configuration so that the backup infrastructure can be easily re-created if necessary.
- **Cost Management:** In an Azure environment, there is a cost associated with nearly everything that you do. A good Azure backup solution should be able to provide you with an estimate of how configuration changes or changes to backup jobs will impact your overall costs.
- **Bottleneck Detection:** In a cloud environment there are any number of things that could result in a bottleneck, which slows down backup or recovery jobs. A bottleneck detection feature could monitor things such as worker process wait times, CPU quotas, and storage throttling to see if the environment is experiencing any bottlenecks. If bottlenecks are detected, then the backup product should ideally provide options for reducing or eliminating the bottleneck.

Choose the Right Solution for You: Using the Online Evaluation Worksheet

You can access the Azure Backup Solutions Evaluation Worksheet online at:

goto.cg/3ewZD05

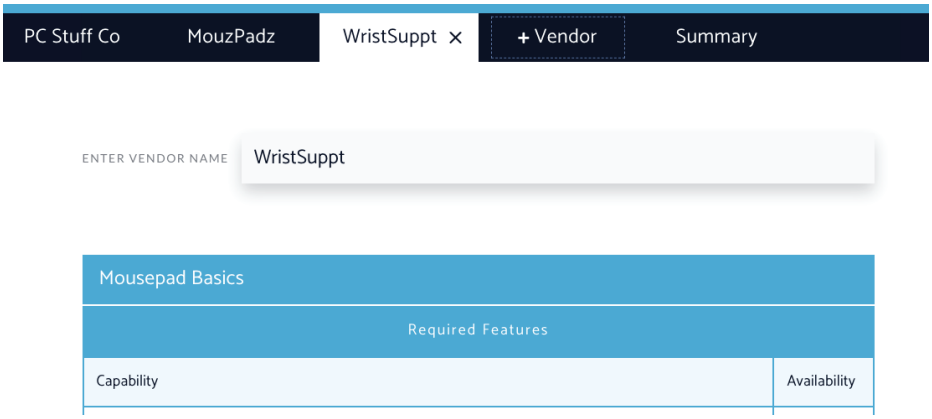
If you'd like instructions on how to use the online Evaluation Worksheet for this Buyer's Guide, keep reading!

Using the Online Evaluation Worksheet

Use the URL provided on the previous page to navigate to the online Evaluation Worksheet for this Buyer's Guide. To use the Evaluation Worksheet, take the following steps:

Step 1 - Add in Your Vendors

Start by filling in the vendors you've shortlisted – you may evaluate up to 5 vendors.



Step 2 – Assess Each Vendor's Solution Capabilities

Each buying criteria set and associated capabilities are represented in the worksheets, split up between *Required* and *Optional* features:

For *Required* capabilities, assess whether these capabilities are available for each solution, checking the box next to each capability under the **Availability** column. For *Optional* capabilities, assign a value in the **Importance** column representing how important each capability listed is to your organization on a scale of 1-10 (with 10 being very important) – doing this one will carry over to every vendor. Then in the **Score** column, assign the solution a subjective score, again on a scale of 1-10, with 10 being the highest. A **Calculated** value will be determined by automatically multiplying each **Importance** value with the corresponding **Score** value. **A Total Optional Score** will be derived from the sum of the **Calculated** values. When done, your worksheet should look something like this:

Mousepad Basics			
Required Features			
Capability			Availability
Ergonomic Design			✓
Memory Foam Wrist Rest			
Non-Slip Base			✓
Optional Features			
Capability	Importance	Score	Calculated
Available in multiple colors	8	10	80
Available in multiple sizes	3	1	3
		Total Optional Score	83

Repeat this process for each vendor.

Step 3 – Review and Download an Evaluation Summary

Click on the **Summary** tab to see how your shortlisted vendors match up:

Mousepad Basics: Required Features			
Capability	PC Stuff Co	MouzPadz	WristSuppt
Ergonomic Design	✓		✓
Memory Foam Wrist Rest	✓	✓	
Non-Slip Base	✓	✓	✓

Mousepad Basics: Optional Features				
Capability	Importance	PC Stuff Co	MouzPadz	WristSuppt
Available in multiple colors	8	32	80	80
Available in multiple sizes	3	18	30	3

Press the **Print Summary** button to download a PDF version of your evaluation.

To learn more, visit ***www.veeam.com***

About the Sponsor

Veeam®, the #1 global market leader in data protection and ransomware recovery, is on a mission to help every organization not just bounce back from a data outage or loss but bounce forward. With Veeam, organizations achieve radical resilience through data security, data recovery, and data freedom for their hybrid cloud. The Veeam Data Platform delivers a single solution for cloud, virtual, physical, SaaS, and Kubernetes environments that gives IT and security leaders peace of mind that their apps and data are protected and always available.

Headquartered in Columbus, Ohio, with offices in more than 30 countries, Veeam protects over 450,000 customers worldwide, including 74% of the Global 2000, who trust Veeam to keep their businesses running. Radical Resilience starts with Veeam.

About the Author

Brien Posey is a 22-time Microsoft MVP, a published author and conference speaker with 20+ years of IT experience, and a Commercial Scientist Astronaut candidate.