Cloud & Service Provider Program

Service Providers: Expand your Portfolio with BaaS for Public Cloud

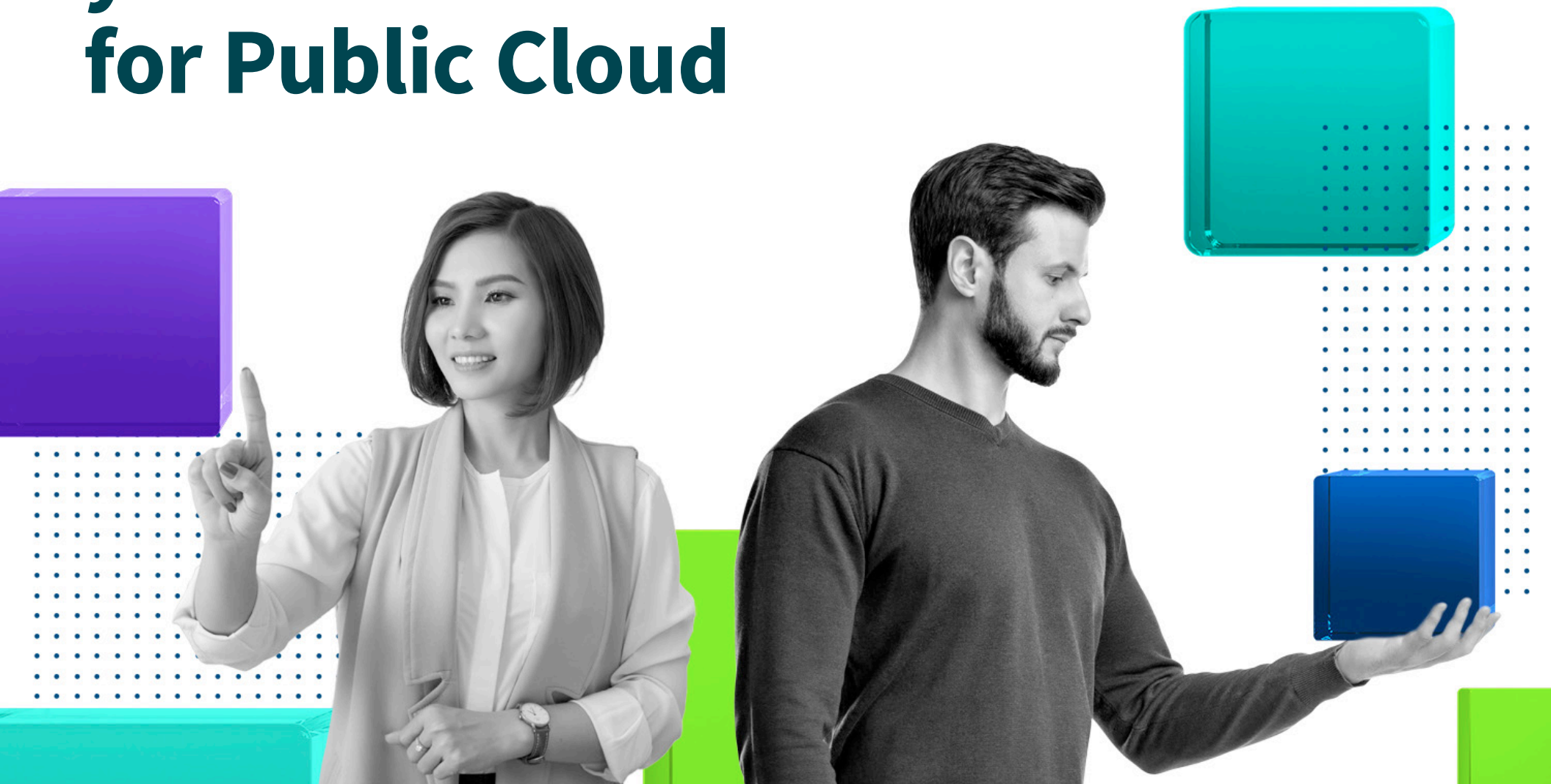

Table of Contents

Even before the pandemic, businesses understood that a hybrid multi-cloud model based on public cloud use could deliver competitive digital transformation business benefits. Today, 83% of organizations agree that hybrid multi-cloud is the ideal approach, with 64% expecting to be operating in that environment by 2023.[1] This hybrid and/or multi-cloud approach to public cloud computing, networking and storage for applications, workloads and data can eliminate crucial challenges like vendor lock-in, latency and higher costs. It can also enable increased regulatory compliance, security, innovation and business resiliency while providing the platform and tools that companies need to scale resources and be agile and flexible with their technology strategy.

Backup and disaster recovery are key benefits of a hybrid multi-cloud approach. More than 50% of organizations will adopt a cloud-centric data protection strategy by 2025.[2] This means that although workloads will remain on-premises and in the cloud, organizations will use cloud resources to manage all data protection activities. However, there are a number of steps for an organization to consider. They must move beyond merely understanding the benefits of cloud backup to understanding how to implement it as a cost-effective and comprehensive system in practice.

Most businesses (55%) anticipate storing their backup data with a cloud provider via backup as a service (BaaS) and disaster recovery as a service (DRaaS) by 2025.[3] This creates an opportunity for MSPs, who traditionally manage on-premises infrastructure. As organizations move to cloud, MSPs are presented with a potentially lucrative opportunity. The key to making the most of this opportunity is understanding the best approach to providing BaaS. This enables the creation of a solid foundation to expand MSP service reach and deliver maximum benefits to the MSP and their customers via public cloud.

83%
of organizations agree that hybrid multi-cloud is the ideal approach

64%
expecting to be operating in that environment by 2023

MORE THAN
50%
of organizations will adopt a cloud-centric data protection strategy by 2025

55%
anticipate storing their backup data with a cloud provider via backup as a service (BaaS) and disaster recovery as a service (DRaaS) by 2025

Hybrid and multi-cloud benefits to business IT

A hybrid multi-cloud strategy based on public cloud gives companies a competitive edge by offering resiliency, agility, and cost efficiency. Specifically, these benefits are derived from the foundations that public cloud provides for IoT, AI/ML, mobility, edge computing, applications and AppDev. More streamlined processes and improved operational insights are a direct result of these, and lead to a better customer experience.

Creating and moving workloads across on-premises data centers and multiple clouds allows for better workload performance and scalable storage options, while simultaneously reducing CAPEX costs. In addition, a hybrid multi-cloud strategy offers agility, flexibility and elasticity of production workloads.

Management across all environments

The need to move, monitor and manage workloads seamlessly across hybrid multi-cloud environments is taken seriously by CSPs. Every hyperscale cloud provider—including AWS, Microsoft Azure and Google Cloud—has developed ways to accommodate hybrid and multi-cloud computing.

On-premises and multiple public cloud options

Today's two CSP market leaders are AWS and Azure, which together capture over half the market (33% and 21%, respectively.)[4] Both providers enable customers to use services like Amazon Elastic Compute Cloud (Amazon EC2,) Amazon Elastic Block Store (Amazon EBS,) or Azure/Microsoft hardware within their own data centers. This provides organizations with flexibility when determining which platform is best suited to run certain workloads and which applications are most suitable for their business.

Leveraging the latest technologies with anywhere, anytime access

Challenges regarding availability, performance and connectivity are commonly faced by distributed organizations working across multiple regions, many of which seek to harness the public cloud benefits presented by edge computing, IoT, AI/ML and analytics in near-real time. Taken together, the latter are crucial for creating and maintaining faster applications and data access near the source. AWS meets that need with 84 availability zones, while Azure has three availability zones per region.[5] Such provision can greatly benefit organizations in navigating multiple iterations of regional data protection and sovereignty laws (which will be discussed later.)

Unending data growth poses both beneficial and challenging aspects for access, storage and backup. According to Statista, the total data growth rate for the average enterprise grew from one to two petabytes in the last two years, a 42.2% annual growth rate.[6] Public cloud placement allows the harnessing the power of that data through access, agile placement and low latency.

Cost optimization of cloud production and backup environments

An added value of leveraging a hyperscale cloud is the ability to optimize costs in production and backup environments. Right sizing cloud environments by identifying mismanaged resources, eliminating unnecessary run times and correctly aligning licensing can lower spend and provide greater performance and efficiency. Scaling up or down infrastructure based on workload requirements can drastically improve consumption and cut costs as well. AWS, Microsoft Azure and Google Cloud provide built-in tools that automate and deliver these optimization services, but there is a learning curve associated with aligning the right tool to the desired outcome.

Another way in which IT departments can improve spend is by negotiating volume discounts and ingress/egress charges with their cloud providers. More consumption equals greater negotiating power—but in order to achieve these outcomes, organizations need to have cloud expertise on staff with knowledge of the built-in cloud tools. This is not always feasible and can result in higher costs.

MSPs bring cloud expertise and knowledge to reduce the complexity of optimizing cloud production and backup environments, while reducing spend and forecasting consistent future costs.

Building cloud services revenue and value

One of the benefits MSPs bring to public cloud and a smart hybrid multi-cloud strategy is BaaS, which provides stability for all other benefits derived from public cloud placement of data, applications and workloads. Many organizations understand the challenges of developing their own backup architecture and approach. BaaS providers can eliminate the expenditure and complexity involved in architecting and managing backup independently.

BaaS solutions collect, compress and encrypt data from applications and workloads across on-premises environments and transfer it natively within the cloud environment or to a third-party provider's cloud-based storage. BaaS providers generally support hybrid cloud backup for synchronization of on-premises and cloud data to cloud storage targets. This offers organizations two benefits. Firstly, it frees up resources by eliminating manual processes of backup job creation and scheduling and parameters. Secondly, it provides monitoring, reporting and regular testing to ensure successful data recovery after disruptions.

Educating customers on the best approaches to backup that fits their needs offers MSPs the opportunity to provide solutions that speak to customer challenges regarding backup implementation and the need for management and monitoring that removes complexity, risk, the need for expertise and uncontrollable costs from the equation. However, without a clear strategy and unified backup solution for customer data in the public cloud, MSPs will struggle when it comes to providing customers with appropriate backup options.

MSP challenges of managing customers' data protection in the public cloud

Organizations are pushing ahead with digital transformation across increasingly distributed environments via hybrid multi-cloud strategies. This has led to challenges of data backup that have increased proportionately to growth of data quantity and data types. Management and oversight of backup in these complex environments is a major challenge for MSPs who must come to grips with the manual processes and a general lack of automation that characterize hybrid multi-cloud environments.

With multiple types of data stored across multiple data centers and public clouds, organizations may struggle to bridge gaps in their backup approach. According to the third-party unbiased report, nearly 90% of respondents say there is a major gap between affordable data loss after an outage and data backup frequency. The implication is that organizations are not meeting their own backup needs, with potentially dire consequences in the case of an outage.

As organizations are increasingly becoming aware of the challenges and pitfalls of implementing, managing and monitoring their own backup, MSPs are presented with a growing opportunity to take on customer data protection. However, MSPs themselves face challenges when it comes to protecting data, workloads and applications across a highly distributed public cloud environment; the burden is simply passed from organizations to MSPs. For MSPs specifically, the challenges inherent in hybrid and multi-cloud backups are compounded when taking on backup management and monitoring for multiple organizations across distributed environments.

There are seven primary data protection challenges that MSPs face—each one explained in depth in this section—relevant both when serving their existing customers and acting as potential roadblocks to customer base expansion. These are common within distributed environments wherein MSPs must find an efficient, attractive and cost-effective approach that wins over prospective customers by dealing with all seven challenges effectively.

1 Cloud sprawl

As hybrid multi-cloud strategies are put in place using public cloud, organizations will find it increasingly difficult to maintain visibility and control over their various cloud platforms, accounts, instances, identities and services. Typically referred to as "cloud sprawl," this common problem can stem from ways of using and accessing the public cloud, including:

- Shadow IT, that is, unchecked SaaS collaboration/communication implementations across departments and divisions without the knowledge of the IT department
- Use of multiple cloud platforms
- Hosting potentially thousands of identities and data instances
- Spinning up and down instances/developer environments
- Sheer data growth and data type expansion across all public cloud environments
- Cloud sprawl results in a lack of data transparency in terms of location, access and use. Cloud native approaches and AppDev bring new applications and workloads, while departments increase unchecked as-a-Service use leading to shadow IT. This poses a major problem even for MSPs using management and monitoring tools, which often leave application, workload, or dependency gaps.

2 Regional data sovereignty laws

Data sovereignty is the concept that digital data is governed by the laws of the country where it is stored. This is a growing challenge in a hybrid multi-cloud world, with organizations operating across regions and storing their data with cloud providers across the globe based on factors such as cost, accessibility and security—and not necessarily with consideration to the relative strengths and weaknesses of local digital data laws.

Sovereignty laws are designed to protect the PII, PHI and PCR data (at rest and in transit) of its citizens via data protection laws. This leads to regulated backup solutions and strict retention requirements for the business or organization that holds that data. The result is that a single organization's data often resides in varied locations with strict regional storage requirements, making data management difficult both for organizations and for MSPs providing backup.

Hyperscale clouds—like AWS and Azure—have many regional zones for infrastructure, compute, data storage and networking, via IaaS, PaaS and SaaS, in order to accommodate access and abide by local sovereignty laws. This is a potential nightmare for MSPs in terms of visibility and management of backups.

3 Shared responsibility and regulatory compliance

Organizations know that they must have complete and comprehensive backup capabilities, but many are unsure of what protections AWS, Azure and comparable services provide. Others are confused regarding the shared responsibility model under which cloud providers operate, which usually state that the provider will protect their own applications and infrastructure, but organizations are responsible for data protection. AWS, Azure and Google Cloud all use this model, and are not liable or responsible for data protection.[7, 8, 9]

4 Workload portability

Workload portability is a cornerstone benefit of hybrid multi-cloud strategies for organizations. The ability to move and adapt data, applications and workloads between on-premises and different public cloud environments can influence almost every aspect of business. For business owners, the ability to avoid vendor lock-in can decrease operational costs, as well as TCO and CAPEX. The potential for ease of scalability and operational efficiency are also appealing for longer-term business goals, as is the improved ability to meet regulatory compliance requirements. Workload portability allows businesses more readily to deliver a superior customer experience through improved services and product delivery and to reach more customers through improving market share.

MSPs are not arbiters of their customers' decisions, including their need for, and implementation of, workload portability. However, MSPs are responsible for considering the impact of portability on how they manage and monitor backup.

Format compatibility and retrievability bring APIs into the picture, thus adding a layer of complexity because the interfaces and APIs of cloud services are not standardized across different providers. Take Amazon API Gateway and Microsoft Azure API Management, which are designed for their respective environments, but are not the same as one another. Additionally, PaaS, IaaS and SaaS can have different levels of interoperability across different CSPs and providers.

5 Multi-tenant remote management and monitoring

Scalability, visibility, resource optimization and streamlined management are key goals for MSPs in multi-tenant backup for their clients. The primary challenges that interfere with achievement of those goals stem from the different backup solutions, needs and visibility presented by different customers. Costs, risks and personnel time are thus increased, potentially resulting in diminishing margins. Collectively, these factors make it difficult to keep existing customers and simultaneously build a sound case to present the MSP's services to new customers, with each new customer exponentially increasing the complexity of an MSP's operations.

Streamlining setup and managing backup for different customers with multiple dashboards can present sysadmins with a mountain of alerts, including false positive and duplicated alerts. Another major concern is the broad lack of visibility into on-premises and cloud environments. This also applies to instances, VMs, servers, applications, workloads, storage databases and files.

6 Licensing complexities and rigidity

Backup providers bring different approaches to licensing, which presents visibility challenges. This is true for component, module-based and instance-based licensing with variable durations and inflexible bundle limitations. Partnering with a vendor that provides a portable licensing structure in a pay-as-you-go model enables service providers to scale up and down as needed, while only paying for the licenses needed. Standardizing backups across multiple environments increases flexibility and makes licensing easier to track.

7 Cost calculating and capacity planning

The previous six challenges contribute to difficulties in cost estimation for MSPs. Different backup approaches, needs, providers and licensing make it nearly impossible to standardize costs and obtain full transparency, both for customers and MSPs.

Cloud sprawl, workload mobility, data sovereignty and regulatory compliance needs make capacity planning difficult, which feeds back into cost calculation complexity. Various clients may work in different cloud environments and use diverse combinations of AWS, Azure and Google Cloud. The result is that visibility, planning based on shared responsibility models, management and monitoring can quickly get out of hand.

MSPs can turn these challenges into opportunities by educating potential customers on these aspects of shared responsibility and the cost of downtime. For example, Veeam's 2022 report shows the following:[10]

- The average outage lasts 78 minutes.
- Downtime tolerance of up to one hour is reported by 56% of "high priority" and 50% of "normal" applications.
- Downtime costs are estimated to be $1,467 per minute, which equates to $88,000 per hour.
- By changing their approach and understanding of BaaS and DRaaS possibilities, MSPs can change the game in ways that facilitate customer and income growth based on streamlined public cloud backup management and monitoring.

Changing the game for managed BaaS and DRaaS in hybrid and multicloud environments

Providing BaaS and DRaaS to multiple tenants is certainly a challenge, but simultaneously can provide an opportunity for business growth. With the right approach to BaaS and DRaaS, MSPs can harness the challenges of hybrid and multi-cloud environments to capture new customers and increase profits.

Single-platform approach

Businesses need application mobility, while MSPs need visibility into those changes. Using a single platform is the only way to support these different needs, and additionally simplifies backup management by enabling the management, monitoring and protection of data, wherever it resides.

A single-platform approach enables agile control and transparency, which delivers cost optimization to the MSP that can then be passed on to the customer. MSPs can deliver customized backup, regardless of infrastructure type or workload, without having to manage a disparate array of vendors or platforms.

Immutability

Immutability — the concept of data whose state cannot be changed — is paramount to ensure that backup files cannot be altered in any way, whether maliciously or accidentally, thus ensuring optimal security and protection from attacks. Immutability offers MSPs additional benefits:

- Simplification of hybrid multi-cloud data protection (customers' data protection mechanisms, whether in the data center, private cloud or public cloud)
- Tool integration and consolidation
- Flexible licensing model that fits a recurring revenue structure
- Full automation via PowerShell or RESTful API

These are key aspects of a scalable, multi-tenant management business model that drives new customer and financial growth with predictable costs.

How MSPs win financially with centralized, multi-tenant management

As MSPs scale up and gain additional customers, it can quickly become confusing, complex and time consuming to manage several different customer backup solutions. The solution is to partner with a single backup service provider that offers a comprehensive, multi-tenant option, making it easy to manage and monitor multiple customer backup environments separately using a single platform and dashboard UI. This gives the MSP the control needed to offer their customers efficient, off-site data protection, reducing costs and management time.

An MSP BaaS solution should provide detailed customizable reports through a single dashboard that visualizes accurate, customer-specific alerts. In addition, it should offer the ability to create, manage and customize separate client profiles through a single portal, including customer-specific:

- Information
- Specifications and requirements
- Backup policies and schedules
- Data retention policies
- Client privileges allocation
- Infrastructure assignment, per customer requirements

These are key aspects of a scalable, multi-tenant management business model that drives new customer and financial growth with predictable costs.

Capacity planning and forecasting tools are also important for meeting each customer's needs. Comprehensive monitoring, analytics and data collection across hybrid multi-cloud environments are necessary for ensuring visibility into virtual and physical data protection environments. RESTful APIs should also integrate into existing platforms and workflows.

An important aspect of this approach is sourcing universal licensing that fits the needs of the MSP and its customers. MSPs can then meet subscription or perpetual option needs across hybrid multi-cloud environments. Ideally, the licenses should be transferable and future-proof for movement across VMware, Hyper-V, Windows, Linux, NAS, AWS, Azure and Google Cloud, since this enables a low total cost of ownership (TCO) for the MSP and their customers. The license should enable post-policy-development viewing of approximate monthly cost projection directly in the UI, which enables future elasticity and scalability based on budgetary constraints to be managed even before process initiation.

Summary: Hallmarks of the ideal backup vendor for MSP customer growth

This e-book has explained the needs of, and challenges for, organizations regarding public cloud backup in the age of digital transformation and hybrid multi-cloud architectures. MSPs are on the front line when it comes to architecting, managing and monitoring backup solutions for clients across every possible environment to ensure maximum uptime and security.

Meeting these goals requires the ability to identify the right vendor to support varied needs, allowing MSPs to build a viable and profitable multi-tenant backup approach that leads to customer growth and profitability.

When looking for a backup vendor, MSPs should include the following in their checklist:

1. Single-pane-of-glass RMM dashboard with multi-tenant visibility into all protected environments; on-premises, cloud and SaaS
2. OPEX licensing in a pay-as-you-grow model
3. Vendor-neutral and hardware-agnostic platform
4. Ability to meet individual client service level agreement (SLA) requirements
5. Robust APIs for seamless integration into third-party software to allow additional capabilities
6. Data, application, workload backup across cloud, virtual, physical and SaaS

7 MSP-centric tools to broaden service offerings and scalability

8 Business intelligence and analytics

9 Single-pane-of-glass RMM dashboard with multi-tenant visibility into all protected environments; on-premises, cloud and SaaS

10 Resource relocation for cost savings and efficiency

11 Detection of performance or availability issues in each customer's applications and infrastructures at-a-glance

12 Dedicated partner program to support MSPs and provide maximum time-to-revenue

MSPs face myriad choices for BaaS and DRaaS that must give them the control and agility to provide optimum customer services and experiences, giving MSPs a market edge on their competition. Veeam offers MSPs backup solutions and programs designed specifically for their changing needs.

Summary: Hallmarks of the ideal backup vendor for MSP customer growth

This e-book has explained the needs of, and challenges for, organizations regarding public cloud backup in the age of digital transformation and hybrid multi-cloud architectures. MSPs are on the front line when it comes to architecting, managing and monitoring backup solutions for clients across every possible environment to ensure maximum uptime and security.

Meeting these goals requires the ability to identify the right vendor to support varied needs, allowing MSPs to build a viable and profitable multi-tenant backup approach that leads to customer growth and profitability.

When looking for a backup vendor, MSPs should include the following in their checklist:

1. Single-pane-of-glass RMM dashboard with multi-tenant visibility into all protected environments; on-premises, cloud and SaaS
2. OPEX licensing in a pay-as-you-grow model
3. Vendor-neutral and hardware-agnostic platform
4. Ability to meet individual client service level agreement (SLA) requirements
5. Robust APIs for seamless integration into third-party software to allow additional capabilities
6. Data, application, workload backup across cloud, virtual, physical and SaaS
7. MSP-centric tools to broaden service offerings and scalability
8. Business intelligence and analytics
9. Single-pane-of-glass RMM dashboard with multi-tenant visibility into all protected environments; on-premises, cloud and SaaS
10. Resource relocation for cost savings and efficiency
11. Detection of performance or availability issues in each customer's applications and infrastructures at-a-glance
12. Dedicated partner program to support MSPs and provide maximum time-to-revenue

MSPs face myriad choices for BaaS and DRaaS that must give them the control and agility to provide optimum customer services and experiences, giving MSPs a market edge on their competition. Veeam offers MSPs backup solutions and programs designed specifically for their changing needs.

Achieving data protection across all environments including the public cloud

Veeam® supports partners with the technology and programs to deliver Veeam-powered solutions in order to meet their customer's data protection needs. With a simple, flexible, reliable and powerful platform, Veeam enables partners to deliver BaaS and DRaaS solutions that inspire customer confidence and loyalty.

Veeam delivers end-user security and architecture control so that MSPs can create both single and multi-tenant environments. With an API-driven architecture that uses native snapshots, storage options and security bolstered by universal immutability, Veeam meets every customer data backup and recovery requirement — whether on-premises or in the cloud. Veeam's solutions are designed to protect any size business from large enterprise organizations down to SMBs.

MSPs supporting the backup and recovery needs of their customers' AWS, Microsoft Azure and Google Cloud workloads must be able to keep data protection persistent to these cloud-native platforms for fast recovery times and data consistency. The ability to move data across clouds or back to the data center with ease is also a desirable capability to better meet SLAs and ensure data is available where and when it's needed. With Veeam Data Platform, MSPs can standardize data protection across any infrastructure — virtual, physical, SaaS and the public cloud — to guarantee data availability.

Veeam Service Provider Console is a powerful, centralized user interface, purpose-built for MSPs that accelerates productivity and scales service offerings all in one place. Veeam Service Provider Console provides:

- Multi-tenant serviceability
- Customer onboarding and billing
- Easy licensing and usage reporting
- APIs and automation
- Customer self-service capabilities

By supporting rather than competing with partners, the Veeam Cloud & Service Provider (VCSP) program delivers the technology and support that grows your business, bottom line and customer trust. Once established, partners can apply for the VCSP Competency Program, which recognizes and differentiates your Veeam offerings within your area of expertise and accelerates your data protection business even further. Your customers demand affordable, flexible and agile protection, which Veeam has delivered to countless service providers and customers across the globe.

Veeam solutions for service providers

Join the VCSP Partner Program

[1] "Vansonbourne, 4th Annual Nutanix Enterprise Cloud Index, https://www.nutanix.com/enterprise-cloud-index

[2] IDC, Worldwide Data Protection as a Service Forecast, 2022–2026: Continued High Growth and New Opportunities, #US49720522, November 2022

[3] Veeam, 2023 Data Protection Trends Report, January, 2023, https://go.veeam.com/wp-data-protection-trends-2023

[4] Bill Doerrfeld, "Majority of Apps Will Use Cloud-Native Development By 2023." Container Journal, June 9, 2022, https://containerjournal.com/features/majority-of-apps-will-use-cloud-native-development-by-2023/

[5] Statista, "Statista Worldwide Cloud Infrastructure Services Vendor Market Share worldwide from 4th quarter 2017 to 1st quarter 2022," https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/#:~:text=In%20the%20first%20quarter%20of,with%20eight%20percent%20market%20share

[6] Alexander S. Gillis, David Carty, "Definitions Availability Zones" TechTarget, https://www.techtarget.com/searchaws/definition/availability-zones

[7] Petroc Taylor, "Total enterprise data volume worldwide from 2020 to 2022, by location," Statista, May 23, 2022, https://www.statista.com/statistics/1186304/total-enterprise-data-volume-location/#:~:text=From%202020%20to%202022%2C%20the,the%20data%20will%20be%20stored.

[8] Terry Lanfear, Ann Marie Hitchcock, "Shared Responsibility in the Cloud," Microsoft,10/05/2022, https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

[9] AWS Cloud Security, "Shared Responsibility Model, AWS, https://aws.amazon.com/compliance/shared-responsibility-model/

[10] Veeam, 2002 Data Protection Trends Report, February 22, 2022, https://www.veeam.com/wp-data-protection-trends-report.html

[11] Google Cloud Architecture Center, "Shared responsibilities and shared fate on Google Cloud," https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate

