

FEBRUARY 2019

**NEC BACKUP AS A SERVICE REDUCES ADMINISTRATIVE TASKS, HELPING IT DEPARTMENTS HELP THEIR ORGANIZATIONS**





## CLOUD MATURITY MAKES BACKUP SERVICES A VALUE-ADDED BENEFIT TO BUSINESS

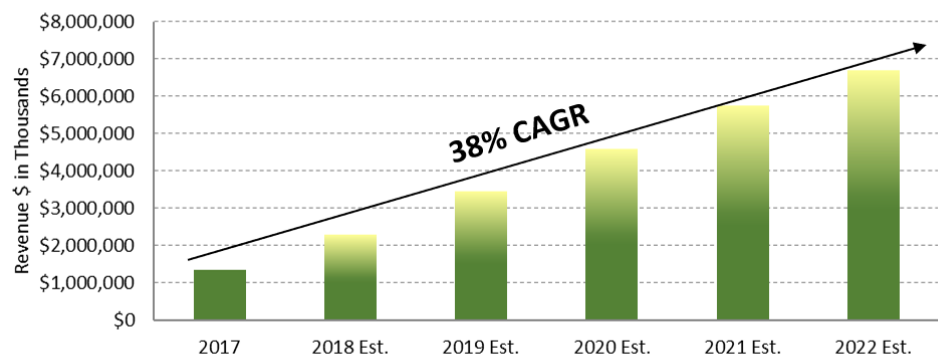
Cloud solutions continue to grow not only in adoption but also in importance in customer IT strategies. In typical risk-averse practices, cloud solutions were initially used near the fringes of IT environments, delivering test and development functions far outside most of the core mission-critical workloads sustaining internal and external business operations. Likewise, customers in regulated industries such as healthcare or government were initially wary of the security and performance of services delivered from third-party data centers. These dynamics are changing rapidly, however, as both the customer and vendor behavior around cloud have matured considerably. Cloud providers have expanded their data center locations, added almost every flavor of regulatory compliance, and enhanced security capabilities. These developments have dramatically lowered the traditional barriers to cloud adoption, allowing customers in almost any industry to have at least the possibility of deploying most of their workloads through cloud delivery methods.

With cloud solutions more secure, compliant and available than ever, customers are faced with maintaining a workload selection process that optimizes their choice of delivery methods. This selection and sourcing strategy is an emerging area of maturity for customers as IT organizations shift from having a builder’s mindset to that of a

concierge. Delivery method decisions are not being made solely on cost, but also around the skills, core competency, and opportunity cost for each workload. An area of emerging consideration, which can provide not only cost benefits but also more strategic value for IT organizations, is the data backup and protection function. The maturation of cloud has created both a need for a new type of protection for data in cloud environments and has also led vendors to develop a solution, as backup solutions can now be delivered in an “as a Service” model through cloud data centers. As customers grow their cloud environments, the need to secure, back up and properly manage the volumes of data being delivered through third-party environments has also grown. The move to utilize different compute instances from on-premises to global multicloud instances can add a great deal of complexity to the underlying monitoring and maintenance of the enterprise compute instance. Additionally, cloud has emerged as a viable option to deliver those same security, backup and management functions regardless of whether the data resides in on-premises, public or private cloud environments. Many IT departments look to off-load basic administrative functions to a third-party provider or to automated control planes that can simplify this task work. Turning to third parties for this basic administrative support frees up internal IT labor to assist the lines of business (LOBs) on higher-value services work and provide better data protection to the overall organization.



### CLOUD BACKUP AS A SERVICE REVENUE MARKET FORECAST



SOURCE: TBR ESTIMATES AND COMPANY DATA



## **DIGITAL TRANSFORMATION ADDS IT COMPLEXITY; MANAGED SERVICES CAN ADD SIMPLICITY**

The rate of change keeps accelerating, challenging IT organizations to keep pace with the required skills and training. Digital transformation opens new markets to enterprises where changes in public policy can require quick technology updates to maintain operations in compliance with local regulations. These challenges impact not only end-user applications and services but also the entire technology stack supporting their delivery. In this way, the backup solutions required to protect against data loss, intrusion and cyber threats add yet another element of complexity requiring continual IT management, monitoring and updating. Keeping abreast of these issues does not add differentiating value to an enterprise. Similarly, the expertise is often something an enterprise does not need on a full-time basis. For these reasons, an increasing number of customers are turning to partially or fully managed cloud offerings. The addition of managed services may increase the cost, but they offer significant advantages over unmanaged “as a Service” offerings, which provide the benefits of cloud delivery but still leave significant risk to the customer for overall performance and data protection. Whether for end-user applications, disaster recovery, or backup services, the core offering and vendor-supplied expertise and management, procured together, are becoming an attractive value proposition. Turning to a managed service provider for that expertise, such as an automatic upgrade to a software control plane that keeps your enterprise operations in legal compliance, offers immense value to an IT staff. The managed service provider can offer a level of business assurance costing pennies on the dollar when compared to the potential cost of data recovery or the fines incurred for failing to comply.

## **DIGITAL TRANSFORMATION JOURNEYS WORK BEST WHEN ENTERPRISES THINK BIG, YET START SMALL**

Discussions of digital transformation often paint a picture of a rapid end-to-end change in technology and process within organizations. As leadership at almost any organization will attest, however, actual changes often take place incrementally and with much greater difficulty than this vision. The rate and pace of technological change can only proceed as fast as the slowest learner in the enterprise. And, for every visible change to customer or end-user experience, there are a multitude of less visible changes required from an IT perspective. At the core of almost any change that IT delivers is consideration for how data will be used, secured and protected from incident. The more the business automates, the more data the business generates, and the costlier data loss becomes to the ongoing operation. Furthermore, the rise in data privacy as an impact on brand means the attention executive leadership is placing on backup and disaster recovery increases. Working with a managed service provider can assure the executive leadership that IT is keeping an eye on mitigating business risks by turning to trusted providers for these tasks while focusing the company’s IT staff on collaborating with business units to optimize and grow the business.

## **NEC BUILT AN ECOSYSTEM TO DELIVER A HOST OF PREMIUM BACKUP AND DISASTER RECOVERY SERVICES WITH MULTIPLE ENTRY POINTS FOR THE ENTERPRISE**

NEC continues expanding the continuum of backup and disaster recovery services it can provide to its end customers through ongoing collaboration with best-in-class technology vendors. NEC’s core partner providers include:

- ✓ **Intel®:** No technology discussion can start without mentioning Intel being at the core. Offering the de facto industry standard, Intel’s world-class technology Xeon® processor and Optane™ persistent memory



technologies are utilized by NEC to provide a rock-solid infrastructure foundation on which the company can layer its proven suite of software utilities, tool sets and dashboards for self-service provisioning through to a fully managed service. Staying in tight alignment with the Intel product road map means NEC can provide best-in-class storage provisioning as Intel hardens and further innovates upon its Optane persistent memory framework in the ensuing years.

- ✓ **Iron Mountain®:** NEC has partnered with one of the venerable names in backup services for decades, Iron Mountain, to deliver a suite of backup and disaster recovery services. Integral to the relationship is NEC's utilization of Iron Mountain's two main data centers through which NEC can provide both backup and disaster recovery services.
- ✓ **Commvault:** NEC utilizes Commvault's full suite of backup and disaster recovery services.

### NEC HAS THE BACKUP SERVICES TO MITIGATE TODAY'S RISKS, AND HAS A FUTURE-PROOF PLATFORM FOR TOMORROW

Oftentimes IT executives are challenged to evaluate the total cost of their existing backup methods against a fully managed service such as NEC's new offering. In addition to the common challenges IT organizations face in providing backup and recovery services, there are hidden costs that do not necessarily factor into the self-managed Infrastructure as a Service offering. Common challenges IT organizations face within the backup domain area include:

- ⊗ **Unreliable or incomplete backup provisioning:** Many firms have multiple backup software applications which run within their environments, oftentimes at the discretion of the end users themselves. Lack of standards can result in the loss of highly valuable information. Similarly, the amount of time dedicated to relearn these provisioning dashboards and gain passing familiarity with each independent software alternative can bog IT staff down.
- ⊗ **Sprawling incremental costs:** In addition to employee labor time spent on ad hoc backup provisioning and responding to LOB requests for data recovery assistance, businesses can also suffer from:
  - Incomplete or partial backups
  - Slow turnaround time moving to cold storage, such as tape backup, versus more rapid and complete restoration from a complete backup copy in the cloud
  - Higher costs associated with maintaining the internal backup systems
  - Higher license and maintenance costs for on-premises backup software rather than access to best-in-class backup software through NEC's managed service offering
- ⊗ **Service levels:** Physical pickup and delivery of backup tapes and the turnaround time to restore information add cost, not just in terms of the internal IT labor associated with this highly manual process but also in the hidden costs to the business from the data loss or security breach.
- ⊗ **Compliance:** Penalties for noncompliance can be severe. Mitigating that risk by hiring specialized expertise versus subscribing to that expertise through a managed service can also be a far costlier solution to the ever-evolving set of public policy statutes around data privacy.

Similar to these issues, most of the challenges do not revolve around the physical storage product, but rather around the business rules and the harnessing of technology innovation to assure an always-on, always-available environment for business users. The costs of losing data, losing business activity awaiting the restoration of that data, and complying with regulatory requirements are not bundled into base-level IaaS backup availability for self-managed support. Cloud platforms such as Amazon Web Services (AWS) and Microsoft Azure may not provide the entire solution customers need, but they can offer a valuable component of the overall backup environment. Being able to leverage the capability, multiple regions and locations, and scalability of storage services like S3 and Glacier from AWS as a backup target can hold



significant value for customers. Savvy customers will recognize, however, that these cloud services along with the efficiency costs of in-house administration versus a managed service providing “one to many” knowledge transfer from subject matter experts through managed services can be a far more economical approach to protecting your company’s data assets.

## **A FULL-SERVICE DISASTER RECOVERY SOLUTION MAY SEEM EXPENSIVE, BUT IT COULD BE SUBSTANTIALLY LESS THAN THE COST OF DOWNTIME**

As business moves to digital underpinnings, the costs of unplanned downtime will only increase. As you consider the costs associated with a more robust backup and disaster recovery plan, honestly calibrate the following:

		
<b>The cost of an hour of unplanned downtime to your business</b>	<b>The number of unplanned hours of downtime your business has had in the past year</b>	<b>The incremental cost of enhancing your backup and disaster recovery provisioning</b>

At a 99% uptime instance, this still translates to a little under 90 hours of unplanned downtime. If that downtime costs your enterprise \$40,000 in unanticipated costs, then your total risk exposure would be \$3.6 million. How does that risk exposure compare to the incremental costs of an enhanced backup and disaster recovery plan?

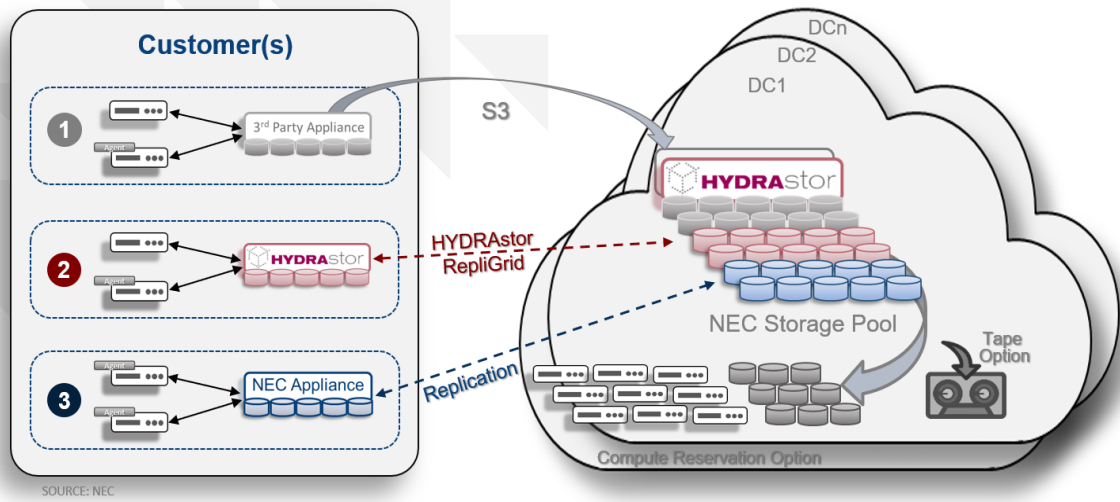
## **NEC’S SERVICE SUITE RANGES FROM SELF-SERVICE BACKUP TO FULLY MANAGED BACKUP AND DISASTER RECOVERY SERVICES**

There is no one-size-fits-all solution for the variety of enterprise compute instances. The NEC service offerings allow enterprises to start anywhere along the backup and disaster recovery product continuum. The core elements of this services suite contains the following:

- ✓ **An NEC on-premises appliance** can allow enterprises to consolidate their older backup technologies onto a hyperconverged infrastructure platform powered by Intel for self-service backup. The appliance provides greater software simplicity and lower Total Cost of Ownership (TCO) by allowing IT departments to retire technical debt associated with dated backup technologies.
- ✓ **An NEC managed service backing up to Iron Mountain data centers** allows for rapid backup provisioning across the entire IT instance into Iron Mountain’s secure, underground data center facility. Full data protection with more rapid restoration times than physically transported tapes for restoring the business operation only increases in importance as more and more revenue flows from digital interactions with customers and suppliers.
- ✓ **NEC trusted cloud targets** allow clients that seek to store critical off-premises data utilizing industry-standard protocols, such as AWS S3 and others, to take advantage of the security and advanced services to lower operational costs.



- ✓ **An NEC/Iron Mountain disaster recovery service** not only preserves the data in the NEC/Iron Mountain cloud but also allows for compute and network resource reservations required to restore the data to operation in the event of a disaster. Additionally, replication to a secondary NEC/Iron Mountain site is as a highly secure replication option for long-term archiving.



SOURCE: NEC



## MAKING SENSE OF BACKUP SOLUTIONS REQUIRES ASKING VERY FUNDAMENTAL QUESTIONS ABOUT THE BUSINESS OPERATIONS

Businesses everywhere struggle to grasp the value and hidden costs of the rapid acceleration in technology innovation, adoption, and the volume of data generated. Understanding what to protect and how to protect it, both for the business and for the regulators, can be a challenge for even the largest of enterprises. But as companies work through these challenges, it is vital to remain focused on the core cost factors and assign as honest a cost comparison as possible in making the decision. Some of these core questions include:

- **What are the current operating costs for the backup provisioning and how much of the internal assets are covered by this process?** Older backup technologies have maintenance costs associated with them that can be removed from the operating budget. Backup as a Service can also free internal staff to work on higher-value business problems technology can address.
- **What is the economic cost to the business when data goes missing?** This is not limited to the amount of time it takes to have a tape transported to the data center and loaded back onto the live system by internal staff. The cost also has to be calibrated for the line of business that idles or performs workarounds awaiting the data restoration.



## CONCLUSION

Given the rising costs of computer outages to digital businesses, customers should consider modernizing their backup solutions at the same time they modernize core IT services. Cloud-delivered services play a large role in both initiatives, not only providing cost benefits but more importantly providing services that simplify IT administration. Cataloguing the current costs of backup and disaster recovery services is vital only as a calibrating starting point when seeking a new approach to backup and recovery. Customers have more options than ever to consider when determining their new IT infrastructure architecture and service levels to empower their strategic business objectives. Many are finding the underpinning backup and disaster recovery decisions equally as strategic and important as the business process changes. Change is difficult and time consuming for many IT organizations based on the breadth of infrastructure, software assets, and managed services available in the market today.

NEC is a provider that recognizes both the opportunity for customers in modernizing backup and disaster recovery services as well as the variety of choices customers seek in building their own solution. Customers should consider NEC and its network of partners, who together have built a portfolio of offerings that can address the entirety of customer requirements. NEC provides customers choices across the continuum of self-managed to fully managed solutions, with partners to help throughout the lifecycle. The breadth and depth of the offerings make NEC a vendor worth considering.

## ABOUT TBR

Technology Business Research, Inc. is a leading independent technology market research and consulting firm specializing in the business and financial analyses of hardware, software, professional services, telecom and enterprise network vendors, and operators.



Serving a global clientele, TBR provides timely and actionable market research and business intelligence in formats that are tailored to clients' needs. Our analysts are available to further address client-specific issues or information needs on an inquiry or proprietary consulting basis.

## FOR MORE INFORMATION

TBR has been empowering corporate decision makers since 1996. For more information, visit [www.tbri.com](http://www.tbri.com).

This report is based on information made available to the public by the vendor and other public sources. No representation is made that this information is accurate or complete. Technology Business Research will not be held liable or responsible for any decisions that are made based on this information. The information contained in this report and all other TBR products is not and should not be construed to be investment advice. TBR does not make any recommendations or provide any advice regarding the value, purchase, sale or retention of securities. This report is copyright-protected and supplied for the sole use of the recipient. ©Contact Technology Business Research, Inc. for permission to reproduce.