MSP BACKUP REPORTING AUTOMATION & OPTIMIZATION

BOCADA

INTRODUCTION

Once upon a time, supporting IT Operations for enterprises was fairly straightforward. Each organization had a limited number of hardware and software tools, and they looked to MSPs to manage these tools efficiently and support smooth business operations. Reliability was the priority. Expertise was the value-add. And enterprises trusted MSPs to ensure systems were implemented and managed correctly.

The current story, however, is quite different.

Enterprise IT operations are increasingly complex. They are juggling legacy backup systems with new technology, internal business requirements with external government regulations and expectations for new revenue-generating projects with a drive toward automation. Data protection and governance is only becoming more challenging. Yet this very challenge is what can help MSPs transition from tactical players to true strategic partners.

> **Data protection and governance is only becoming more challenging. Yet this very challenge is what can help MSPs transition from tactical players to true strategic partners.**

Helping customers navigate complex backup environments while reducing their costs gives you a chance to offer real customer value. By offering proactive and automated backup reporting for operations, management oversight and audits, MSPs can elevate their standing in the eyes of enterprise organizations. Data stays safe, sound and compliant. You delight, retain, and grow major accounts.

DATA PROTECTION AS IT WAS

Compared to today, data protection was once relatively straight-forward. Limited product and storage choices on a finite number of sites and geographies, coupled with clear expectations from enterprise customers, made data protection an important but tactical endeavor. Reactive approaches to backup and customer service allowed MSPs to deliver backup services with minimal scrutiny. However, with the advent of digital transformation and growing cybersecurity risks, MSPs see their role becoming more strategic.

HANDS OFF CUSTOMERS

Outsourcing data storage and protection to MSPs used to be a way to clear a necessary, but onerous, task off of enterprise IT teams' to-do list. Knowing a dedicated team was tackling data storage and protection allowed enterprises to remove it from their radar, allowing MSPs to sell a "just trust us" approach to customer accountability.

> **" It used to be that data protection was outsourced, the box was checked, and that was acceptable. "**

With operations handed off and limited expectations or demands for rigorous reporting from customers, MSPs were able to do day-to-day management and oversight with minimal feedback to their customers. It used to be that data protection was "outsourced", the box was checked, and that was acceptable.

REACTIVE CUSTOMER ENGAGEMENT

In this "just trust us" data protection environment, customer service was also reactive. Engaging with customers was limited to responding to crises or inquiries as they came in.

IT was a complex and burdensome function for non-digital Fortune 500's and they were satisfied to have blue-chip technology providers taking care of their needs. There was little expectation that MSPs would anticipate customer queries, let alone have proactive solutions in place to share performance or optimization metrics, giving MSPs few opportunities to share the value they were adding. After all, limited to just being operational partners, customers didn't expect MSPs to bring value-added, strategic solutions to the IT mix.

TAPE & DISC

Tape and disc have historically been the media types of choice for enterprises looking for cost-efficient long-term storage solutions. The downsides of these media types—manual handling, off-site storage, challenging data restoration—were largely accepted since they allowed organizations to meet mandated data retention policies cheaply. MSPs could make recommendations on particular hardware choices, but there wasn't much need for input into the process.

However, as regulatory policies evolve and the need for archived data accessibility grows, new media types are being added to the mix. MSPs now need to balance data stored on tape and disc with data stored in the cloud.

" As regulatory policies evolve and the need for archived data accessibility grows, new media types are being added to the mix. MSPs now need to balance data stored on tape and disc with data stored in the cloud. "

LIMITED BACKUP SOLUTIONS

Historically there was an expectation that a Fortune 500 company would have a homogeneous IT environment. That is, they would pick one vendor from which to buy hardware and the software required to run it. The storage, tapes and servers could be coupled with the backup application offered by that vendor for a tidy environment that included all of an enterprise's data protection needs. It was once a great formula to allow enterprises to simply outsource IT operations and for managed services providers to provide profitable services.

ON-PREM INSTALLATIONS

Installing and managing on-premises data centers was the status quo. Major upfront capex investments were expected for expansive server rooms and the infrastructure—electricity, generators, natural-disaster-rated structures—to support them. As these capabilities became a required but non-core competence for enterprises, MSPs could provide the know-how for these activities including backup processes and data protection operations. This represented a hefty capital investment but a more simplified architecture and set of choices than present-day IT operations managers face.

MANUAL DATA COLLECTION

Backup data software has always generated metadata, allowing IT Ops teams to individually mine each backup server for raw data, download it, compile it, format it and then prep it to be shared across the organization. This is a hyper-manual, time-intensive approach that increases headcount requirements as enterprise data grows. As IT salaries grew and data proliferated, this became a significant cost for a relatively repetitive task. The result was enterprises outsourcing the work, and then MSPs moving the work offshore.

In relatively simple backup environments, this was once manageable. MSP IT Ops teams could become experts in one or two backup software products, becoming fluent in each products' unique scripts and GUIs. The moment backup environments contained three, four or more backup applications—the new normal—the situation, and risk of human error, changed entirely.

" The moment backup environments contained three, four or more backup applications—the new normal—the situation, and risk of human error, changed entirely. "

REACTIVE JOB FAILURE FIXING

With relatively simple backup policies and backup solutions, limited risk associated with data loss, and far fewer compliance and government regulations, real-time or near-time reporting was generally not prioritized. Further, with extremely limited options for holistic oversight, back admins were forced to wait for complete backup cycles to run before pulling metadata.

In this type of environment, it could take days to discover a job failed. As a result, troubleshooting and re-running failed backup jobs was once the status quo.

REDUCE BACKUP FAILURES BY 72%

With backup performance data in one place, you can identify problems before they causes crises—and reduce monitoring and reporting time.

Source: Bocada case study

DATA PROTECTION AS IT IS

Today's backup environments are more complex and harder to manage than ever before. The introduction of cloud storage, the presence of multiple backup applications, and the demands for increased governance and compliance across a wide range of stakeholders is making the everyday job of safeguarding data more prone to risk and error. Of course, this is all happening within a landscape that features growing cyber security threats, increasing government regulation and end-customer demands for more and more services at no incremental cost.

This perfect storm means one thing is truly critical for MSPs: they must find efficient ways to raise their data protection game by automating governance and compliance reporting to free up IT Operations personnel to focus on other strategic initiatives.

FRAGMENTED BACKUP ENVIRONMENTS

Enterprise data protection environments fragment for a variety of reasons. Some enterprises grow through mergers, acquisitions and geographic expansion, and their backup environments become increasingly complex with each expansion. Others migrate from one technology or technology vendor to another as new capabilities come to market. Multiple backup software products comprise these fragmented backup environments, each with unique data collection protocols, GUIs, and scripts. This drastic fragmentation makes it harder and harder for MSPs to exercise efficient governance over outsourced data protection operations.

CYBERSECURITY & RANSOMWARE

Recent ransomware and cybersecurity attacks increase the stakes for data protection and recoverability. The NotPetya and WannaCry ransomware attacks have shown the globally debilitating scale these malicious efforts have on commerce and data security while also showing the inherent risks of not having appropriate data governance procedures in place.

These external threats are making recoverability plans all that more relevant. MSPs need to prove that backup operations comply with data security policies and data is readily recoverable in the event of an attack.

> *This perfect storm means one thing is truly critical for MSPs: they must find efficient ways to raise their data protection game by automating governance and compliance reporting to free up IT Operations personnel to focus on other strategic initiatives.*

CLOUD STORAGE & DISPERSED BACKUP

With enterprises moving data to AWS, Azure and other public and private clouds, data becomes more dispersed and a whole new range of data protection scenarios take shape. Tapes, discs and on-prem servers continue to play a role in holding critical historical data. But, with companies increasingly leveraging cloud storage to retain data, juggling storage types is that much more challenging. Additionally, with Azure native backup capabilities and AWS snapshots, the number, type and location of backups extends well beyond the traditional data center.

As the shift to the cloud accelerates, MSPs will be expected to support a complex range of backup environments from cloud-native to hybrid to on-prem. Having a systemic way to monitor data operations, no matter where they live, will be critical for MSPs looking to effectively and efficiently oversee complex environments for their end customers.

GOVERNMENT COMPLIANCE REQUIREMENTS

Government regulations are ever changing, and growing more sophisticated and complex. 2018's introduction of the General Data Protection Regulation (GDPR) makes it crucial to know what data is available, and be able to show where it is stored and how long it is retained. GDPR is just the newest addition to the countless existing regulations like HIPAA, FFIEC, FINRA and more.

As MSPs manage the globally-stored data of multinational organizations, they are expected to fulfill regulatory compliance obligations for their customers. Adapting to the nuances of each regulation and ensuring that data protection aligns with the relevant policies will increasingly be expected as part of any MSP's data backup services delivery.

DATA VISIBILITY DEMANDS

Stakeholders need broad data protection visibility. Executive leaders, internal and external auditors, government regulators and, of course, storage and IT Operations personnel all need different levels of detail and transparency to verify data security compliance.

When faced with delivering reporting on such a diverse range of information—backup performance and success rates, storage trends and capacity usage, performance to SLA goals, compliance with federally-mandated regulations—MSPs have a unique challenge: finding ways to efficiently and effectively deliver relevant reports... in a timely fashion.

> *As the shift to the cloud accelerates, MSPs will be expected to support a complex range of backup environments from cloud-native to hybrid to on-prem.*

DECENTRALIZED & FRAGMENTED BILLING

Managing data protection oversight for multiple customers means managing billing for multiple customers as well. Cost structures negotiated customer-by-customer, ranging from billing for total number of clients backed up during a time period to billing for backup storage used or even by unique business units or geographies under management, can lead to hours spent each month on billing alone. Regardless of the structure, enterprise customers expect transparency and auditable billing reports.

Without an objective method of determining how to bill customers, teams regularly face recurring, time-intensive activities and may receive regular pushback from enterprise customers looking for additional details to validate the invoice they receive.

INCREASED SERVICE AT LOWER COSTS

The sum of the growing complexity and expectations for service delivery—proactive reporting, digital transformation, meeting compliance obligations, leveraging new technologies, anticipating customer needs—creates huge challenges for MSPs. And yet, despite these growing expectations, enterprises also demand greater efficiency. Customers expect MSPs to offer more for the same or lower costs.

Finding efficiency through automation of repetitive and time-consuming activities is the only way MSPs can balance growing functionality and value-add while lowering the marginal cost for customers.

" Finding efficiency through automation of repetitive and time-consuming activities is the only way MSPs can balance growing functionality and value-add while lowering the marginal cost for customers. "

WINNING THE DATA PROTECTION SPACE

MSPs are now faced with a major challenge: becoming a full-service, strategic partner to customers while simultaneously adapting to growing complexities in the data protection landscape.

Using tools to centralize, streamline and automate that complexity is the only way for MSPs to continue delivering the same caliber of service while reining in the every-growing recurring, time-intensive activities that grow headcount costs and pull their teams away from other high-value activities.

UNIFIED MONITORING OF DISPERSED BACKUP ECOSYSTEMS

Leveraging a scalable solution that aggregates data across backup applications and storage devices in cloud and on-prem environments removes hundreds of labor hours from outsourced backup operations.

This all makes data protection monitoring a centralized, one-stop-shop and removes the need to staff account-specific teams with countless individuals who only specialize in particular backup solutions. MSPs get organizational efficiency and team members get to work on higher-level activities.

DECREASE BACKUP CAPACITY NEEDS BY 50%

Daily storage reports are automatically delivered to the right people, helping you make the most of your resources and minimizing the need to purchase excess backup capacity.

Source: Bocada case study

STREAMLINED REPORTING

A major time-saving opportunity is automating report creation. Once data is aggregated automatically, having a system that consolidates it in easy-to-visualize ways and lets you adjust it to your needs, like sorting backup successes and failures by server, geography, backup product, etc, makes oversight seamless. Backup admins can more efficiently hone-in on issues that leave end customer data unprotected and fix them before they affect billing or SLA goals.

This frees up teams to do ad-hoc reporting as customer inquiries come in, and also gives them the opportunity to do proactive reviews of customer environments and offer ways to optimize performance and usage—just the value-add an enterprise customer is looking for. By streamlining reporting, MSPs can create opportunities to deliver higher levels of service while still maintaining highly tuned operations.

By streamlining reporting, MSPs can create opportunities to deliver higher levels of service while still maintaining highly tuned operations.

AUTOMATED COMMUNICATION

Faced with an ever-growing list of stakeholders requiring unique information, automating the distribution of tailored reports becomes a must-have for MSPs looking to share data in a timely fashion.

By pre-scheduling report distribution on a daily, weekly, or monthly basis, customers are ensured regular updates, getting the information they need to gain confidence in data protection practices and the broader regulatory and compliance guidelines are being met. Meanwhile, MSPs get to take a time-intensive, sometimes human-error filled task, off their to-do list.

HYBRID CLOUD PROTECTION

Enterprise customers are moving more of their IT operations to the cloud. In fact, they might already have their backups there. They are looking at digital transformation efforts to drive revenue growth while keeping overhead costs down. MSPs must have an efficient way to bridge the divide between legacy and cloud operations. By equipping backup teams with automated ways to oversee on-prem and cloud backup activities, not to mention data retention policies on legacy storage devices like disc and tape, MSPs will be ready to support next-gen initiatives while not losing sight of legacy operations and data governance requirements.

By equipping backup teams with automated ways to oversee on-prem and cloud backup activities, MSPs will be ready to support next-gen initiatives while not losing sight of legacy operations and data governance requirements.

ALERTING, TICKETING AND REAL-TIME STATUS

Moving from reactive to proactive data protection and governance oversight means having backup operations integrated to capture performance activities as they happen. However, no backup admin can efficiently monitor thousands upon thousands of backups along with the residual messages and actions they create. Instead, leveraging a tool with alerting, ticketing integration and real-time backup performance provides admins with an effective, efficient way to focus their attention on results and performance enhancements.

Teams are now empowered with a way to jump on data protection issues, helping them meet and exceed SLA goals every month.

CENTRALIZED BILLING & REPORTING

Pulling the necessary information for regular customer billing can take hours each and every month, yet it must be done in a timely manner since backup applications typically purge metadata each month. With a systemized and automated way of extracting customer-level data and the relevant billing criteria for each customer, like number of back ups or amount of data backed up, teams can remove countless labor hours from billing oversight and billing report generation.

Further, automating the distribution of this information to finance teams gives them easy-to-understand data that lets them bill on time, and in a way that customers will understand and accept.

CONCLUSION

MSPs looking to offer additional value to enterprise customers while safeguarding teams from incremental, onerous tasks are well served by introducing automated backup data reporting and monitoring. It's a proven method of protecting data while ensuring sustained customer satisfaction.

Organizations evaluating the best approaches for implementing backup reporting and oversight automation—from in-house, custom development to 3rd party tools—will want to consider solutions that address compliance, systems oversight and reporting in one single platform.
This includes solutions that:

- Automate backup data collection and data normalization across cloud and on-prem backup environments
- Automate backup performance reporting and ease failure troubleshooting
- Enable action-oriented information sharing with internal and external teams
- Allow for customizable reporting for unique compliance criteria
- Segment backup environments into useful reporting groups
- Provide real-time visibility for proactive backup performance monitoring
- Offer systems and storage performance metrics

Joining these capabilities in a single solution will play a key role in making data protection and recovery planning not just simpler for backup and storage teams but also more efficient, better securing customer data and driving long-term customer satisfaction.

DISCOVER WHAT BOCADA CAN DO FOR YOU

Bocada LLC, a global IT automation leader, delivers backup reporting and monitoring solutions that give enterprises complete visibility into their backup performance. Bocada provides insight into complex backup environments, enabling IT organizations to save time, reduce costs and decrease risk.

With the largest installed customer base in the Fortune 500, Bocada is the world's leading provider of backup reporting automation.

To try Bocada in your backup environment, contact us at:

sales@bocada.com

425-898-2400

⟩BOCADA.