

# Automating Backup

Opportunities & Best Practices





# Introduction

You already know that backing up your organization's data isn't a nice-to-have, it's a need-to-have. The external threats alone warrant this. You could be one of the 50% of all organizations operating a data center that can't withstand, or is unable to operate after, a natural disaster.<sup>1</sup> Or, you could be one of the 39% of global organizations that experienced a ransomware attack in recent months.<sup>2</sup>

If those threats weren't enough, you're likely accountable to a host of government regulations that legally require you to back up your data and be able to report on the fact that you're doing just that. The Gramm-Leach-Bliley Act's Safeguard Rule requires that sensitive customer information be archived securely while Sarbanes Oxley's Section 404 requires companies to not only document the procedures in place to safeguard data but also to make sure it's available for reporting on an annual basis. If you're doing business in Europe, the EU's 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 it is being retained. In short, you have a lot of laws telling you not just to store your data, but to prove you are storing it and storing it correctly.

But reporting on data backup storage is getting harder and harder. Organizations are expecting 52% data growth in the next twelve months.<sup>3</sup> Yet a global IT data protection labor shortage means the manpower simply doesn't exist to implement and manage this massive growth in data.<sup>4</sup> And, even if the manpower existed, flat or shrinking IT budgets won't support incremental hiring.<sup>5</sup>

Suppose resources weren't an issue, employee morale and retention would still be a priority. The repetitive acts associated with backing up data and reporting on it time and time again are bound to disengage team members you can't afford to lose.

All of these reasons point to why automating your data protection reporting matters. Time-intensive, repetitive tasks that must be completed are far better left to software and automation than to manual processes that take precious time and resources away from higher priorities like security. When you automate your backup reporting, your organization gets the data protection assurances it needs and your team gets to work on higher-value, engaging projects.

## Backup Reporting Automation Best Practices

When automating backup activities, there are two core areas where streamlining operations will reduce man hours, no matter where you store your data:

**I. Automating Operations:** These are the day-to-day activities that give your team daily oversight over data protection and ensure that you're meeting internal policy objectives.

**II. Automating Compliance:** These are the regular activities that demonstrate compliance and keep key stakeholders informed.

When automated in tandem, these two areas decrease labor overhead, help move your team to more value-add projects, and reduce the risk of data loss.

# Automating Operations

Manually overseeing the day-to-day tasks associated with backups is time intensive. Between regular scripting, managing multiple backup products, analyzing backup performance across regions, and balancing backups on tapes, disks, and the cloud, there is no room left for additional work. However, automating these steps vastly reduces time and human error from the equation. The following provides a list of key categories of operational data protection activities that can be automated.

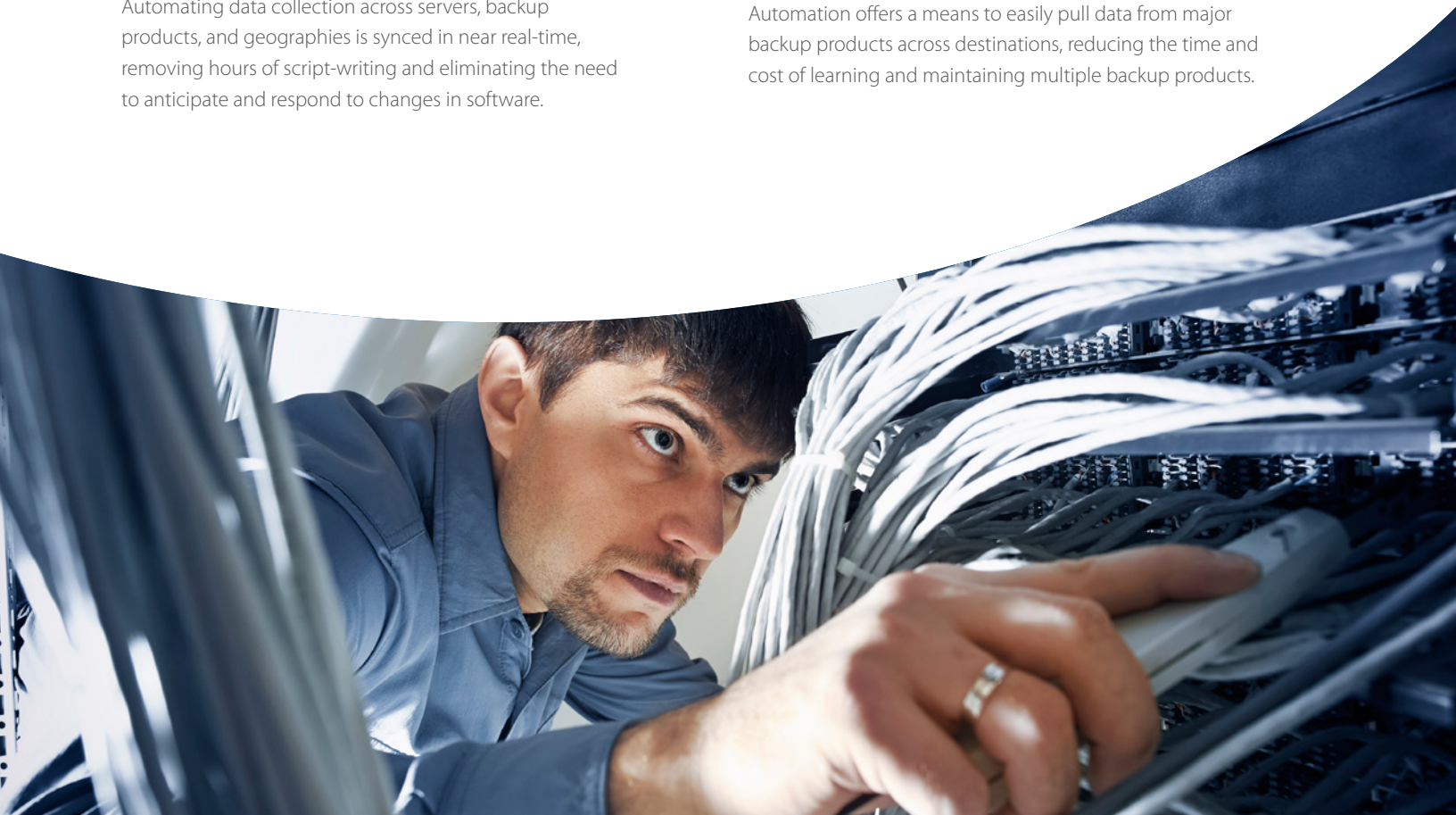
## Data Collection & Reporting

In enterprise organizations, the process of running scripts across servers to read relevant backup metadata on everything from backup load and throughput to the success or failure status of backups is daunting when you consider how many clients you're backing up spread across business units and geographies. Couple this with OS and backup server updates that can make those scripts obsolete as well as needing to normalize data in digestible formats on a regular basis and you're left with a hyper-manual, error-prone process.

These processes can, and should, be automated. Automating data collection across servers, backup products, and geographies is synced in near real-time, removing hours of script-writing and eliminating the need to anticipate and respond to changes in software.

## Consolidated Reporting Across Backup Products & Destinations

In organizations that have undergone mergers and acquisitions, or even just technology evolutions, it's typical to juggle different backup products as well as different storage options like Data Domain, StoreOnce, Azure, or AWS. Using native reporting tools or worse, manual reporting, means writing scripts unique to each product and destination, and usually having multiple individuals in-house who specialize in each backup product's GUI, scripting and native reporting tool. Likely, that detail then needs to be consolidated into a unified report on backup performance at an enterprise level. Automation offers a means to easily pull data from major backup products across destinations, reducing the time and cost of learning and maintaining multiple backup products.





## Enterprise Reporting Across Departments, Geographies or Customers

What do you do when you have thousands of clients being backed up, spread across geographies, departments, business units or customers? It's often ideal to review backup performance at those unique levels, but manually slicing and dicing backups into discrete groups takes time.

By sectioning your environment's clients or servers with distinct naming conventions, you can automate reporting to isolate particular reporting categories. Segmenting anything from departments, geographic regions, or even customers is now a cinch.

## Backup Success Monitoring

At the most fundamental level of backup reporting is the classic high-level view of how servers, clients or targets are performing. When you find yourself always asking yourself, "What percent of backup jobs were successful, and what percent were not," you're in a situation that's ripe for automation. Receiving a daily report with comprehensive success and failure data from jobs run overnight eliminates hours of repeated script writing and gets you the answer right away.

## Backup Failure Reporting

Anyone working in the data backup space knows that one backup failure is rarely cause for alarm. However, recurring failures is another thing entirely. Automating the isolation and compilation of consecutive failures lets you know it wasn't a one-off event that caused those failures but rather a larger issue that needs to be investigated. On top of that, automating the aggregation of consecutive failures by error type can take you from an ad-hoc job-fixing approach to a systemic, time-saving process.

## Capacity Management

One likely culprit behind backup failures is storage capacity. Without insight into how much disk space is used and how much is available for backups, your backups could easily fail based on insufficient disk, tape or cloud storage capacity alone. Yet, when you consider how much time is spent on fixing job failures, it's tough to devote additional hours to disk utilization and occupancy too.

Automated monitoring of storage utilization can quickly alert you to create more capacity for your next round of backups. Or, it could be the evidence you need to request more storage.

## Job Failure Alerts & Ticketing

Why spend time looking to see if key backups failed? Why not be alerted about failed jobs...and have a service ticket immediately opened in your system to tackle the issues?

Automate job failure alerting and ticketing instead. By programming email alerts that tell you which key backup failed, when it failed, and the error associated with the failure, and then syncing that information with your ticketing system, admins have the foundational information they need to fix the problem. This shortens the time spent identifying and logging failures, and decreases the time spent on failure troubleshooting.

## Retention Policy Tracking

Different types of data have different retention policies, some driven by industry regulation and others driven by internal policies. Keeping tabs on the seemingly infinite amount of data stored off-line or in the cloud, and the retention periods of that data, can be overwhelming. Yet, it's critical to verify and document that you are adhering to proper retention policies.

Automating data retention expiration reporting can take charge of an onerous, yet necessary, task. You can tackle data deletion when necessary, and spend your time more efficiently when you don't.





# Automating Compliance

Saving time and manpower on operational processes is just one place automation matters. Once you tack on the compliance and communication requirements of data reporting—sharing information with internal stakeholders and auditors, cost allocations, communicating with customers—you'll see how automation can truly drive resource efficiencies. The following provides a list of key categories of data protection compliance and audit reporting that can be automated.

## Report Distribution

Consider everyone in your organization that needs to see backup reports: the core backup team and department heads as well as internal and external auditors, just to name a few. That's a lot of different groups, each of which expects different information.

Automating report distribution means reports will get you out of the reporting communication and distribution business. Your stakeholders get the information they need, in the format they expect, and you don't have to touch a thing..

## Audit Documentation

The amount of time spent with auditors understanding failure issues, and reporting on the resolution, can feel endless. When auditors isolate a particular client or server to explore, it can mean looking back through months of history to re-create and understand the issue in question and what was done to resolve it.

Using a system to capture and store the proverbial paper trail allows backup teams to knock out two birds with one stone: documenting the steps taken to resolve failures and making it easy to find and share exactly what those steps were with auditors.



## Policy & SLA Compliance

What SLAs do you have in your organization? Perhaps you need to meet certain backup requirements like a full back up every day, or an incremental backup every day coupled with a full back up every week. Or, perhaps you're expected to have 98% of all backups succeeding at any given time. Reporting on SLA compliance is often mandatory, but takes time away from operational tasks.

Automate pulling reports configured to your unique SLA requirements. Marry this with automating sending reports to internal and external audit teams and you'll enjoy streamlined SLA reporting at a fraction of the time.

## Auditing

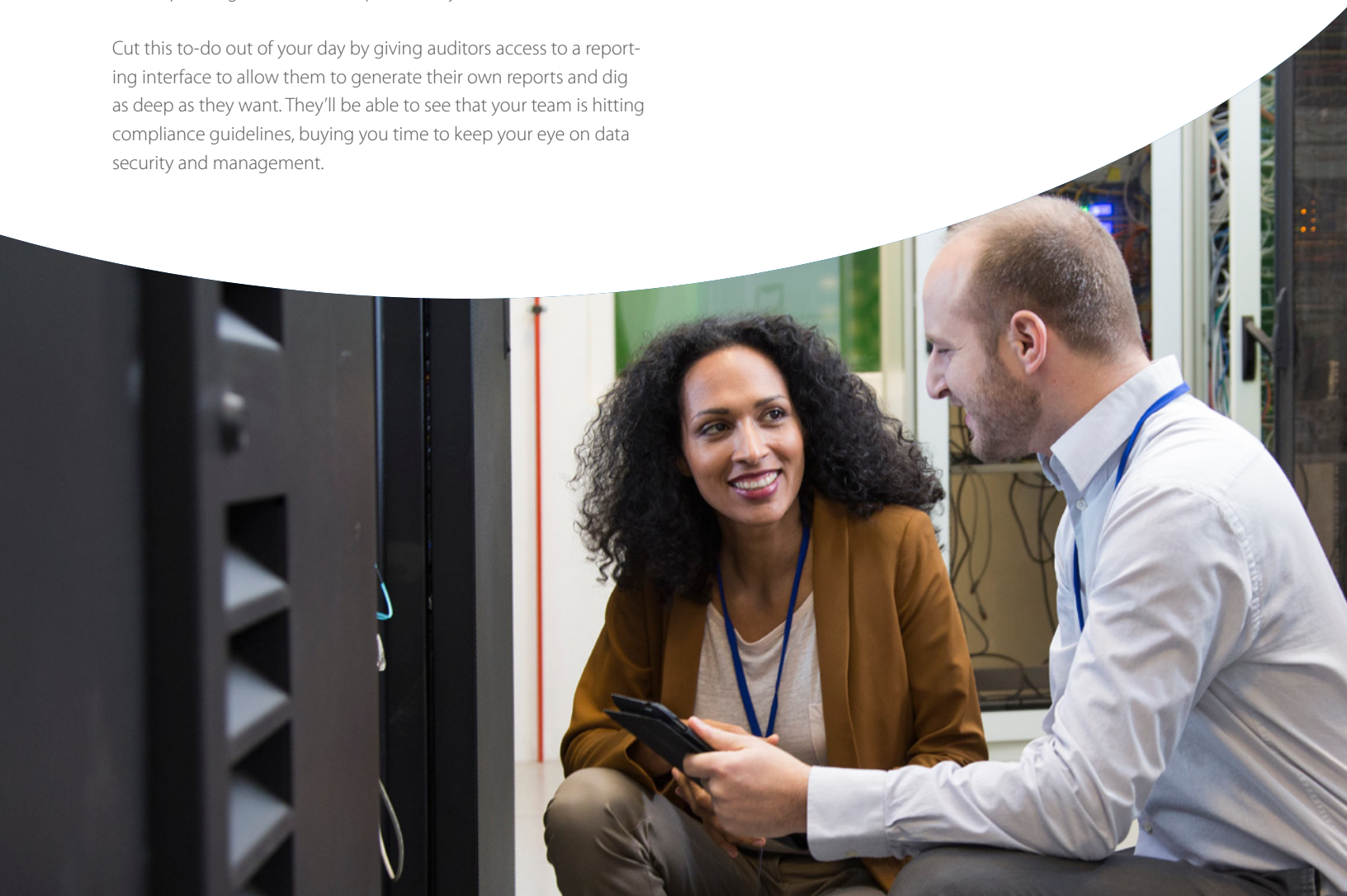
Even after you've automated report creation and distribution, as well as SLA compliance tracking, you're still left interfacing with auditors and responding to their data requests. But you don't have to.

Cut this to-do out of your day by giving auditors access to a reporting interface to allow them to generate their own reports and dig as deep as they want. They'll be able to see that your team is hitting compliance guidelines, buying you time to keep your eye on data security and management.

## Budgeting & Cost Allocation

At a time when you're looking to decrease IT costs, being able to allocate backup usage by department is ideal...if you have a way to accurately allocate costs.

Automating the grouping of servers by department, and then automating reporting by those departments, offers an accurate, time-effective way to determine the share of usage by department, and distribute costs accordingly.





# Conclusion

Backup reporting automation offers a lot of benefits for companies looking to streamline their processes and rein in the time and costs associated with this task. It doesn't just simplify day-to-day backup operations but also the critical information sharing that comes with these responsibilities.

If you're considering automating more of your data protection activities, whether building it yourself or with third party tools, you'll want to select an option that meets your needs across reporting, compliance and capacity planning.

Applying these capabilities to backup reporting efforts will play a key role in making data protection and recovery not just easier but also more efficient, safeguarding your organization and its critical data.

A holistic solution will:

- Function seamlessly across your suite of backup products.
- Reduce or remove manual activities and script writing.
- Offer backup visibility across business functions, business units, and geographies.
- Provide details on stored data volumes at the client and server level.
- Enable action-oriented information sharing with internal and external teams.
- Allow for customizable reporting that adapts to your unique business requirements.

## How Much Money Could Reporting Automation Save You?

Request our free ROI Calculator and see firsthand how much money you'll save on data collection, reporting, troubleshooting and loss with the proper backup reporting automation in place.

[Request ROI Calculator](#)

<sup>1</sup> "Managing Growth, Risk & The Cloud." *Zenium Data Centers*, Spring 2015, [www.zeniumdatacenters.com/en/wp-content/uploads/sites/2/2015/11/Zenium\\_Research\\_Spring2015\\_ExecSummary.pdf](http://www.zeniumdatacenters.com/en/wp-content/uploads/sites/2/2015/11/Zenium_Research_Spring2015_ExecSummary.pdf).

<sup>2</sup> "Understanding the Depth of the Ransomware Problem in the United States." *Malwarebytes*, August 26, 2016, [www.malwarebytes.com/surveys/ransomware/?alid=13242065](http://www.malwarebytes.com/surveys/ransomware/?alid=13242065).

<sup>3</sup> "2016 Data Center Industry Survey." *Uptime Institute*, Feb. 2016, <https://uptimeinstitute.com/publications/asset/2016-data-center-industry-survey>

<sup>4</sup> Steve Morgan, "Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021," *CSO*, June 6, 2017, <https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html>.

<sup>5</sup> "2016 Data Center Industry Survey." *Uptime Institute*, Feb. 2016.

# 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, automate ongoing reporting activities, and reduce costs.

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](mailto:sales@bocada.com)  
+1-425-898-2400

