CODE42

Five Steps to Worry-Free Endpoint Backup & Data Migration

Eliminate data loss risk by protecting all enterprise information

EXECUTIVE SUMMARY

Today's organizations face a ballooning data management and risk problem. The use of laptops, tablets, workstations, servers and smartphones in the enterprise—all from a variety of vendors running various operating systems and software applications—continues to grow.

The amount of critical data created and stored by knowledge workers is growing at an alarming rate, and organizations face increasing pressure to meet new and existing data retention laws and compliance regulations.

Despite these issues, many companies still rely on a legacy, platform-specific data backup solution, even though it doesn't provide consistent backup across the enterprise. This outdated approach becomes especially risky when IT faces a data migration initiative. Whether migrating to a new version or brand new operating system, or to new hardware on either the client or the server—organizations risk immense data loss and an expensive, intensive disaster recovery undertaking if they launch a data migration effort without first properly securing their data.

Continuous, real-time data backup is the only viable solution for protecting all enterprise data while providing for a seamless migration process. But how do you achieve it?

FIVE STEPS TO WORRY-FREE ENDPOINT BACKUP + DATA MIGRATION

Forward-thinking IT teams can effectively address the above concerns and eliminate the data loss risk from data migrations with a comprehensive approach to endpoint backup across the enterprise.

STEP 1: Identify Your Basic Endpoint Backup Needs

As individual workstation and laptop storage capacities grow, efficient data backup becomes ever more crucial. Selecting the right tool for the endpoint device backup job includes evaluating a multitude of factors:

- How much data must be backed up, where will it be stored and how long will it be stored?
- How much time is available for backup?
- Which storage devices are already deployed?
- Is centralized backup administration available?
- Is flexibility for local, centralized, and remote backups available?
- Is the system fully interoperable (any client platform/OS to any server/OS)?
- Is high data integrity maintained?
- Is a self-healing capability included?
- Is the system scalable?
- Is automatic failure recovery included?

All of the above are critical considerations when evaluating endpoint backup solutions. Yet there are additional factors that will not only address your initial requirements, but also enable you to identify a more sophisticated, comprehensive backup solution that empowers end users while easing the burden on IT.

STEP 2: Solve the Pyramid Problem with User Self-Restore

In most organizations, trouble tickets requesting file restore assistance may sit unaddressed for several days due to IT overload, scarce resources, or difficult and costly data recovery.

But this issue can be addressed without doubling IT overhead or putting a data recovery provider on retainer: empower all enterprise users to quickly and easily restore their own data—whichever data they want, whenever they want it—and you eliminate the issue altogether. Any user can recover any file from any location via any Internet connection and any device, with only a few clicks.

STEP 3: Solve the Performance Problem with Block-Level Data De-Duplication

Many enterprise backup solutions utilize basic, file-level data de-duplication—essentially backing up only a single instance of any given file (and assigning pointers to subsequent instances). But this ineffective approach can increase storage costs while slowing backup and recovery speeds.

Block-level data de-duplication, on the other hand, looks inside each file and saves only a single, unique iteration of each chunk of data. A hash algorithm generates a unique number for each chunk of data, then indexes that number. Then, when a file is updated, only the specific data that is new or changed is backed up.

STEP 4: Solve the Security Problem with End-to-End Encryption

To eliminate security risks, select an endpoint backup solution that encrypts data on the client (AES 256-bit), again during transit during backup, again on the server, and yet again during restores.

STEP 5: Develop a New Data Migration Process

So what does an effective, efficient migration process that incorporates comprehensive endpoint data backup look like? Consider this hypothetical operating system and computing platform migration:

- From Microsoft Windows XP to Macintosh OS X 10.8
- Across 500 devices in a business unit
- Includes 100 laptops

In the past, the IT department would roll out upgrades in a series of waves, resulting in frustrated users. This time, the IT director implemented an endpoint backup solution to protect the data stored on those 500 devices. Now, the migration process looks like this:

Desktop support:

- Procures a new iMac and a new MacBook Air from inventory
- Configures, installs and tests all necessary applications—including the endpoint backup client software—and then tests the devices
- Signs off on testing results/configuration recommendations
- Implements any necessary changes and IT director approves
- Creates separate images of the computers' primary storage devices—for the iMac and MacBook Air—then makes appropriate backups
- Deploys the new computers using the images, which are installed during non-business hours

Then, IT restores to the new laptops the most recent version of the users' work directories from the most recent backups, and employees return to work to find their new computers (and all of their data) ready and waiting for them on their desks.

With the above, new, streamlined process, desktop support focuses on the migration rather than troubleshooting backup; the migration process is more efficient; and users enjoy a simplified, trouble-free migration experience.

A SOPHISTICATED SOLUTION FOR ENDPOINT BACKUP BEFORE, DURING AND AFTER DATA MIGRATIONS

CrashPlan

CrashPlan meets and surpasses all of the above endpoint backup needs, giving you a firm foundation for a strategic and seamless data migration process. Engineered to back up endpoint devices—especially laptops—CrashPlan is exceptionally easy to use and manage, helping you implement consistent backup procedures for all users, regardless of their location.

The CrashPlan server operates quietly in the background to provide continuous data protection on all devices. It effortlessly handles backups and restores for an unlimited number of users while verifying backup archives, balancing disk storage, upgrading users and alerting the administrator to any problems.

A "platform-enthusiastic," cross-platform approach protects all users

With CrashPlan, no computer and no department is left unprotected. One solution for all operating systems means IT need only purchase, learn and maintain a single product for enterprise-wide backup.

Continuous, invisible, uninterrupted backup

With CrashPlan, backups run continuously and can be automated or user-initiated, so users don't even have to remember to back up their files. And because CrashPlan is so quiet and unobtrusive, users can continue working without interruption.

Easy self-restore

CrashPlan's self-service restore functionalities significantly speed up the retrieval of backed up data. Users restore files, immediately, themselves—even when away from the office—without involving IT staff.

Secure mobile access

Users can download, view and share files backed up with CrashPlan from an iOS, Android or Kindle mobile device. In addition, downloaded files are instantly available on the device, even when offline, and CrashPlan's special "One-Touch Update" makes it easy to get the latest version—automatically—of all downloaded files while on the go.

A variety of data destination options

CrashPlan doesn't dictate where your data has to be stored. You tell us where you want it—your cloud, our cloud or a combination of both.

Robust, intuitive admin capabilities

CrashPlan's intuitive, real-time dashboard of your entire backup environment—including policies, profiles and data retention—makes managing your backup easier. From the console, administrators enforce data retention policies, ensure compliance, and specify backup timing and security settings. CrashPlan also is self-managed and self-healing.

Superb scaling

CrashPlan scales infinitely due to its inherent flexibility, reliability and efficiency. You can leverage existing infrastructure while meeting your growing needs due to CrashPlan's open architecture. And with its superior compression technology, CrashPlan offers no restrictions regarding file size, versions or archives—yet is able to maintain high efficiency.

End-to-end security

Upon backup activation, data is automatically encrypted (AES 256-bit) before it is saved to a local backup device or transported across the LAN, WAN or Internet. And data remains encrypted during transit and storage. In addition, CrashPlan integrates seamlessly with Open Directory or Active Directory via LDAP, Radius for dual-factor authentication, and Shibboleth/SAML 2.0 for federated, cross-domain single sign-on.

Byte differential data de-duplication

CrashPlan's byte differential/block-level data de-duplication only stores new information, meaning information repeated within a file—as well as information repeated across multiple files—is backed up only once.

Tamper-proof archives via guaranteed restore

CrashPlan's backup verification process checks the health of backup archives days, weeks, months and years after the original data blocks have been backed up, so any user or admin can recover backed up files based on date, time or incremental version. Users can easily search for specific files, and cross-platform restores are supported across any available network medium.

Customizable backup sets

Users can determine which groups of files are sent to which destinations with which backup settings—settings which may be different from or in addition to content IT backs up per policy.

CONCLUSION

Before undertaking a data migration initiative, it's critical to understand and implement a comprehensive endpoint backup solution. Without it, your company's data—its life-blood—is threatened, and you knowingly are engaging in a very real, very expensive, disaster recovery possibility.

CrashPlan software protects everyone in the enterprise—regardless of the number of users or their physical location—with continuous, cross-platform, multi-destination backup. It works quietly in the background, with users continuing to work and usually unaware a backup is even occurring. When they need to restore a file, they're happy to know it's merely a few clicks away, and they can do it themselves, without IT intervention.

With CrashPlan, you have a powerful, flexible endpoint backup solution that provides immediate value today while assuring you of a reliable, effective data migration platform for the future.

DOWNLOAD YOUR FREE, 30-DAY CRASHPLAN TRIAL TODAY!

essentials.code42.com/FiveSteps

OR CONTACT CODE42 SALES

www.code42.com/contact

CORPORATE HEADQUARTERS 1 MAIN STREET #400 | MINNEAPOLIS, MN 55414 | 612.333.4242 | WWW.CODE42.COM