CODE42

The Guide to Modern Endpoint Backup and Data Visibility

Data loss, theft or breach is inevitable

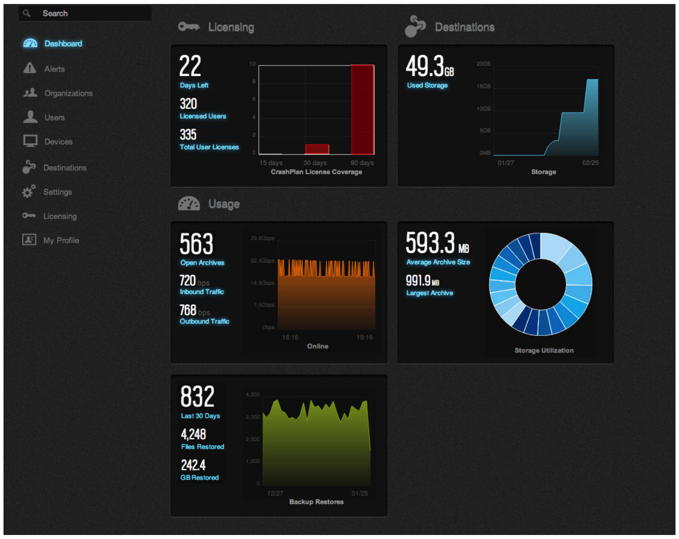
Backup assures recovery, continuity and rapid response

Endpoint data backup is at the core of an enterprise data security strategy. Modern endpoint backup goes well beyond backup and restore, delivering risk reduction across the enterprise and addressing perennial IT and business problems.

Today, endpoint backup is being used to:

- Recover from ransomware
- Accelerate tech refresh and data migration
- Support legal hold
- Meet data privacy and retention requirements
- Provide forensic evidence to mitigate and remediate the effects of a breach
- Identify insider threats via data activity monitoring

What's happening across the endpoints?



Gain visibility and control from a single console. Continuous endpoint data backup gives you complete visibility of the data living on, and moving to and from, your users' endpoint devices.

The erosion of employee loyalty is risky for the organization. Sixty percent of Code42 customers use endpoint backup to secure data in the event of employee departures.

TECH VALIDATE

The 2015 Cost of Data Breach Study by Ponemon Institute reported 60 percent of companies experienced more than one data breach in the previous two years. The average total cost of data breach participating in 2015 Ponemon research increased from $3.52 to $3.79 million.

PONEMON

> "Data security isn't an IT issue, it's a business problem. Information protection and control isn't something you wait to implement until you've been breached."
>
> **Rick Orloff, CSO, Code42**

Make the case for endpoint backup

Speed up, save time, cut costs, recover and remediate fast

Endpoint backup makes life easier for IT staff and makes the enterprise more secure. The right solution offers a single console to manage thousands of users and device types and provides relief or recovery from:

3/4 of companies worldwide fail at disaster readiness.[1]

140,000 hard drives crash every week.[2]

12,000 laptops are stolen every week.[3]

eDiscovery costs an average of $18K/GB[4]

38% of data migrations fail[5]

Disaster. Nearly three of four companies worldwide are failing at disaster readiness. No one wants to think about disasters, but they are a fact of life. Endpoint backup allows an organization to quickly and easily recover when disaster strikes by "rehydrating" data to existing or new devices.

Hardware failure. 140,000 hard drives crash every week. Whether a power surge wipes out a laptop or an encrypted hard drive simply stops working, the best of IT hardware can—and will—fail. Endpoint backup makes it simple for the user or IT to restore files to a new device with minimal impact on user productivity.

Device theft. Endpoint backup provides an accurate and reliable way to identify whether or not a stolen laptop contained reportable data. Endpoint backup provides an up-to-date view of the content on stolen devices enabling IT to quickly determine whether reporting is required (47 states require notification when protected information is breached).

Litigation. Electronically stored information (ESI) is subject to enterprise protection and eDiscovery compliance requirements in the event of litigation. This is typically done via manual data collection and preservation processes. The ability to to apply a preserve-in-place legal hold to end-user files that are centralized and organized by end-user archive makes legal hold comprehensive, fast and far less expensive.

Tech refresh. Transferring user and system files from the old machine to the new machine typically comes with a 38 percent failure rate. The most common issues are unexpected downtime, technical incompatibility, data corruption, application performance and data loss. Not surprisingly, data migration has a tremendous impact on IT and users.

With endpoint backup in place, every file on the retired device is protected before, during and after tech refresh—preventing data loss. And with good self-service tools, endpoint backup can shift the onus of data migration from IT to the end user, and be conducted at the convenience of the end user.

New malware is born
EVERY 4 SEC.[6]

Ransomware. New malware is born every four seconds and discovered malware strains have increased year-over-year by 77 percent. Ransomware is the most notorious of cyber-extortion methods because the ROI for ransomers is high. Once the machine is infected, it encrypts the files and demands a ransom. The FBI advises ransomware victims to pay the ransom if their files are not backed up. However, with automatic, continuous endpoint backup in place, your organization will never pay a ransom.

HALF
of senior managers admit to stealing data when leaving a job.[7]

Insider threat. With access to systems and a bigger window of opportunity, insiders can do more serious harm than external hackers—causing damage as severe as suspension of operations, leak or loss of intellectual property, reputational harm, diminishing investor and customer confidence, and data leaks of sensitive information to third parties, including the media. Endpoint backup enables 100 percent visibility into the content on endpoints and with endpoint monitoring, the movement of data.

The average data breach costs
$3,790,000[8]

Data breach. The fallout and clean up efforts associated with a data breach cost companies across the globe $3.79 million on average. In the United States, organizations paid an average of $6.53 million per instance—often over-reporting the extent of breach because they lack insight into what records existed on endpoints. With endpoint backup, the organization knows with certainty what data resides on a stolen or breached device to rapidly remediate and accurately report.

> “Most users don’t understand the level of risk that they face when they store any kind of data on their computers or mobile devices. User education is key, yet also the biggest challenge.”

Philip Benware, IT manager
Harvard Medical School

What do employees take with them when they go?

Customer information

Sales lists

Discounting policies

Credit card information

Health information

Employee talent and reward models

Financial records

Software code

Email lists

Strategic plans

Product roadmaps

Process documents

Proprietary formulas

Customer databases

Research and development materials

Employees’ personal information

Food, clothing, shelter and endpoint backup

Endpoint data visibility unlocks new capabilities in the enterprise

Maslow’s hierarchy of needs is a theory of human motivation often depicted in the shape of a pyramid with the most fundamental physiological needs at the bottom and increasingly higher-order needs built on top. At the apex is “self actualization,” a psychological state in which an individual has fulfilled each previous level of need—e.g., food, shelter, safety, love, esteem—and is able to reach his or her full potential.

Similarly, when the basic needs of endpoint data protection and redundancy are met, the data set powers other activities in and on behalf of the enterprise.

Modern endpoint backup builds on the data set and gives you more bang for your buck

When all the data is protected on a single platform, additional competencies can be built atop the archive to solve existing and future business problems.

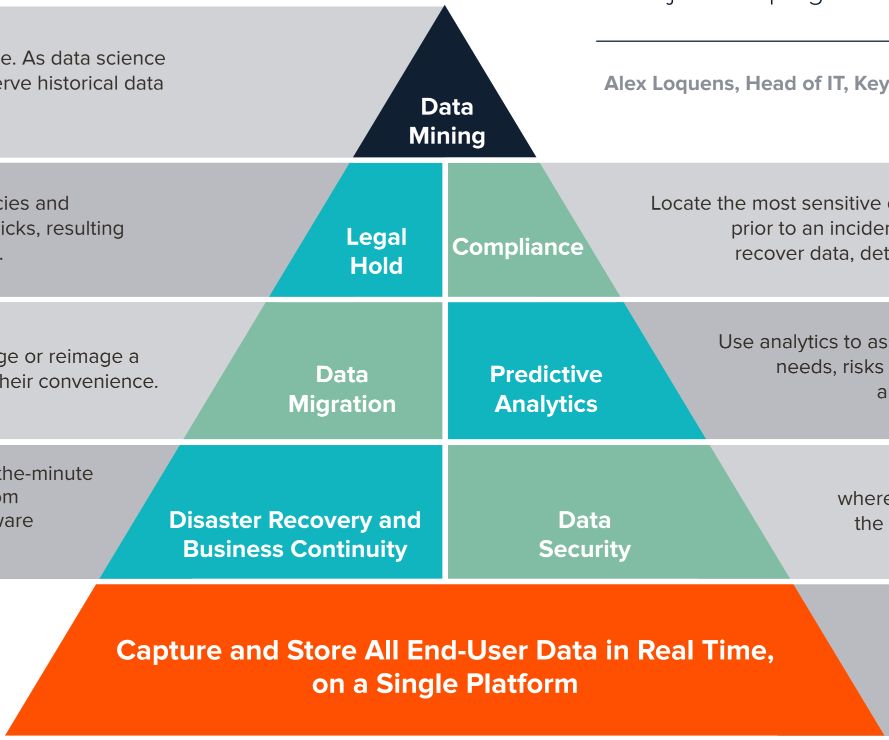
Data migration is faster and foolproof. Legal hold becomes easy to manage. The collected data can be used to derive actionable intelligence—to make the enterprise more secure against insider threats.

Endpoint backup can show you:

- Which employees are uploading which files to third-party clouds
- Which employees have transferred which files to removable media
- Which employees have uploaded which files via web browsers, including web-based email attachments
- Unusual file restores that may signal compromised credentials
- The content of files and folders
- The location of sensitive, classified and “protected” data

Every IT and InfoSec professional today is concerned with doing more with less. With a single backup platform, the need for additional loss prevention, forensic and file integrity monitoring agents is reduced, as is the level of labor, energy and computing real estate on the client.

> “CrashPlan allows us, as an IT department, to focus on new projects and improve the way we operate as a company rather than just keeping the lights on.”
>
> **Alex Loquens, Head of IT, Key Forensic Services**



Turn big data into business advantage. As data science evolves, those companies who preserve historical data will have a certain advantage.

Data Mining

Assign custodians, preservation policies and data collection with several mouse clicks, resulting in tremendous time and cost savings.

Legal Hold

Compliance

Locate the most sensitive data throughout your organization prior to an incident. Support the ability to audit and recover data, detect breach and remediate quickly.

With data migration tools, IT can image or reimage a device and let users migrate data at their convenience.

Data Migration

Predictive Analytics

Use analytics to assess and anticipate the behaviors, needs, risks and aspirations of your customers and clients to fuel business growth.

Restoring data from a healthy, up-to-the-minute backup data set assures recovery from hardware failure, loss, theft, ransomware and disaster.

Disaster Recovery and Business Continuity

Data Security

Security tools provide insight into where data is and where it is moving so the organization can identify potential risks—such as insider threats.

Capture and Store All End-User Data in Real Time, on a Single Platform

Data is encrypted, stored and accessible to end users and IT on a single platform. The data set empowers new capabilities.

Visibility helps you fight insider threats

Recognize suspicious activity, unintentional and malicious behaviors

Research reveals that half of employees keep confidential corporate data when they leave organizations and believe it is their right. When data walks out the door, the organization is at risk of operational, financial, and reputational damage.

UNPREDICTABLE HUMANS: Still the weakest link in data security

Insider threat emanates from unintentional or malicious behavior by employees, former employees, contractors or partners with knowledge of the network and security practices.

78% of security professionals say the biggest threat to endpoint security is negligent or careless employees who do not follow security policies[9]

90% of organizations experience at least one insider threat each month[10]

The average organization experiences **9.3 insider threats** per month[11]

In 2013, U.S. companies suffered **$40 billion** in losses from unauthorized use of computers by employees[12]

Internal actors are responsible for data loss 43% of the time; half of these exposures are accidental, the other half are deliberate.[13]

Accidental Exposure

Shadow IT applications utilized by employees can provide hackers with access points via software vulnerabilities.

Sync and share technology. 28 percent of employees have uploaded sensitive data to the cloud.[14]

Social engineering via phishing, phone, malicious links and physical access are on the rise at companies of all sizes.

PWORD: 1234

Poor password security. Weak passwords, shared passwords and sticky note password reminders substantially reduce security.

Malicious Exposure

Disgruntled employees may delete files or destroy data in retaliation.

Malware infection and logic bombs purposely infect a network with malware or code "bombs" that destroy data at a future trigger date.

Selling corporate data. Some employees seek profit by selling data; others do it to watch their former company burn.

Software updates. Updates—including security patches—are ignored giving hackers a short runway into the network.

With modern endpoint back up, the enterprise will:

- Recognize suspicious employee activities
- Isolate breaches sooner—mitigate impact and cost
- Identify problematic behaviors and the need for end-user education

Support data migration and tech refresh

Make tech refresh painless for users, faster for admins, better for business

The progression of endpoint technology is relentless. Enterprise IT is constantly moving users from old machines to new devices and software, making data migration a critical and time-consuming part of tech refresh—always with inherent risk of data loss.

Each device refresh occupies both IT and the end user for two to three hours—leaving users without a means to accomplish their work and forcing IT staff to dedicate weeks of time to finish large-scale migrations. And when a data migration fails, as 38 percent do, the timeline extends.

Modern endpoint backup enables DIY data migration

A modern endpoint backup solution continuously and automatically moves data from the device to the cloud—and back again to a new machine whenever you need it. The best part? The end user can manage the entire data migration process herself.

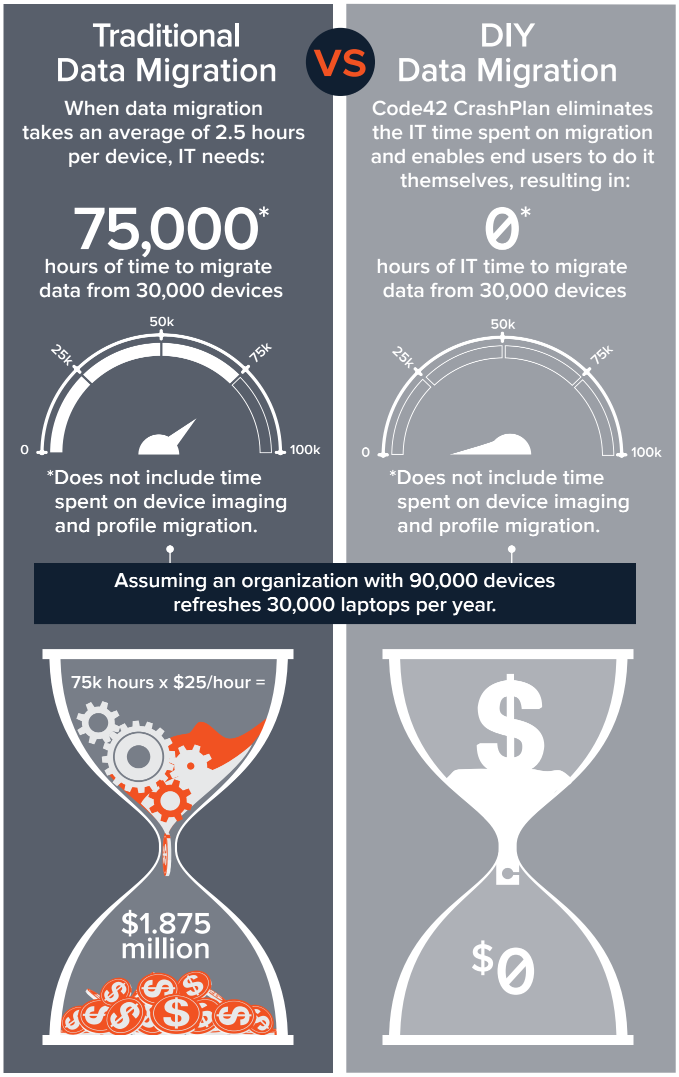
Endpoint backup collects and centralizes user data and organizes it in a user archive—with no requirement for a side-by-side device replacement. Because it's automatic and continuous, there's no need for a time-consuming initial backup prior to migration. The user's archive is already complete. Moreover, after IT images the new device, they can transfer responsibility for data migration to the end user—cutting hours from daily IT schedule and thousands of hours from the overall refresh timeline.

Modern endpoint backup also allows the user to take a customized approach to restoring data on new or reimaged devices. Data can be selectively or entirely restored.

The must-haves when counting on endpoint backup to support data migration include:

- **Automatic, continuous capture of end-user data:** If any information is lost during migration, the user can easily restore the files from the backup files.
- **Streamlined transfer of device settings:** An endpoint backup solution that supports Microsoft User State Migration Tool (USMT) ensures device settings—such as desktop background and network preferences—transfer to the new device.
- **Intuitive navigation and on-screen guidance for dummies:** Self-service migrations are facilitated by a simple interface that offers on-screen help.

Compare the cost savings of do-it-yourself data migration during tech refresh



Traditional Data Migration

VS

DIY Data Migration

When data migration takes an average of 2.5 hours per device, IT needs:

75,000*

hours of time to migrate data from 30,000 devices

*Does not include time spent on device imaging and profile migration.

Code42 CrashPlan eliminates the IT time spent on migration and enables end users to do it themselves, resulting in:

0*

hours of IT time to migrate data from 30,000 devices

*Does not include time spent on device imaging and profile migration.

Assuming an organization with 90,000 devices refreshes 30,000 laptops per year.

Migration costs double when hardware is leased:
If data migration requires a duration of quarantine to ensure all data has been successfully transferred, the organization pays for the decommissioned and the new machine. With an annual rotation of 30,000 machines, double payments add up fast.

> "Code42 CrashPlan delivers on the promise of reliable, fast and secure data migrations. It gives us the automatic, professionalized process that we'd been seeking for so long."

Michael Bowers, team leader of infrastructure at American Fidelity Assurance Company

Reduce eDiscovery costs

Continuous endpoint backup facilitates rapid, accurate legal hold

Litigation has always been expensive, but with the mobile workforce driving an explosion in electronically stored information (ESI), corporations are watching legal costs skyrocket as legal counsel (and IT) work to identify, collect, review and present data for litigation. It's time to take a proactive approach. Continuous endpoint backup works on top of user backup archives to streamline legal hold, simplify eDiscovery and protect your organization from the rising costs of litigation.

When employee devices are backed up, IT has visibility—via historical archive—of every version of every file, wherever employees are stationed.

This approach to legal hold eases pressure on IT and Legal departments and protects the organization from omitting relevant data during production. Most significantly, the proactive process of data protection prevents a reactive process when litigation is threatened and saves the organization many, many thousands of dollars.

> "We welcome the new legal hold tool as it easily allows us to meet legal hold requests as well as put protection in place for departing employees."
>
> **Timothy Basham, IT Manager**
> **Marshall Associates Inc.**

eDiscovery Driving Rising Litigation Costs

4 in 5 U.S. companies have faced litigation in the past 12 months[15]

71% of U.S. companies incur $1M annually in legal costs[15]

43% of larger companies exceed $10M in annual legal costs[15]

eDiscovery accounts for more than **HALF** of litigation costs[16]

Proactive endpoint backup simplifies legal hold

Reduce searched content

Eliminating 100MB of content during the collection phase saves $1,364 in eDiscovery costs.[17]

Reduce employee time

3% reduction in employee time spent on legal hold means >$1M in savings per year.[18]

Reduce overall costs

63% cost savings from proactive eDiscovery.[19]

Recover from ransomware now

When hit with ransomware, endpoint backup supports rapid recovery

File-server backup is great for a predictable, controlled, contained environment that undergoes scheduled backups and updates. But the inevitable has happened. Office employees save information to desktops; mobile workers do the same with laptops; and backup admins have lost control. Add to that, bring your own device (BYOD) and IT consumerization, and the backup market has now shifted to the other end of the spectrum: an unpredictable, multi-OS, de-centralized environment where file servers don't serve.

Servers hold and secure massive amounts of data and are integral to enterprise data governance, but using them to recover lost or damaged files requires time, a trained professional and the patience of a saint. For painless recovery from data loss or malware that encrypts files and asks for ransom, endpoint backup is the clear leader.

WHICH BACKUP BOOSTS RECOVERY?

SERVER BACKUP

To back up to network file servers, users must be connected to the network physically or virtually.

If it's automatic, server backup typically runs once every 24 hours at night when machine resources can be fully utilized—leaving 24 hours of end-user data at risk each day before backup runs.

- The ransomware-infected device is collected from the end user, for diagnosis and re-imaging.
- There is always a risk that the virus was also transmitted to the file server, in which case the files cannot be recovered. (GAME OVER)
- The user is given a loaner device with a few basic tools to use while his or her device is under repair.
- Server backup is unwieldy. Locating and retrieving files is difficult and time consuming.
- Files are manually moved to a new (or re-imaged) device together with standard software.
- User resets his or her device settings and preferences, reorganizes restored files and identifies which files and versions are missing.
- IT explains that as a result of multiple dependencies—backup frequency, IT prioritization and version control—data loss from endpoints is a fact of life.

AUTOMATIC WORKS. POLICIES DON'T.

Despite policies commanding users to initiate server backup daily or weekly,

⚠ **94%** ⚠

of companies surveyed by IDC reported users don't follow policies—putting their data at risk of loss.

WHEN RANSOMWARE STRIKES

When malware strikes, IT and security teams must focus on securing the network and the extent of intrusion before restoring productivity.

ENDPOINT BACKUP

Code42 CrashPlan securely backs up files whenever the device is connected to WiFi.

CrashPlan is a lightweight agent on the device that works automatically and continuously to back up every version of every file to a secure cloud location. Data is encrypted both in transit and at rest.

- The ransomware-infected device is collected from the end user, for diagnosis and re-imaging.
- User's data is stored in a single archive—not cross pollinated with other user's data—which speeds file recovery.
- Personal preferences carry over automatically.
- User gets back to work, even as files are being restored.
- User retrieves all data—except for that produced just moments before ransomware encrypted his or her files.
- IT closes the help desk ticket and goes to lunch.

File sync-and-share vs. backup

Addressing fundamentally different data challenges

Endpoint backup and file sync-and-share software solve two fundamentally different problems and are complementary, not synonymous. Endpoint backup creates a second copy of every file, while OneDrive and other sync-and-share tools store a small subset for sharing among people, teams and geographies. Endpoint backup is automatic and continuous, and it protects all the data on a device regardless of how it's used or shared.

All for one and one for all. What makes sync and share software so powerful is also what makes it dangerous: Edits made to a synced document in real time alter the document in real time. So, for example, if an end user accidentally deletes a critical document on his smart phone, it will be deleted from the archive. If the user discovers his mistake, he can typically go back to the file sync-and-share tool within 30 days to recover the deleted document. If not, it's gone for good.

But only one guarantees easy ransomware recovery. In a ransomware attack, file sync-and-share software would enable an employee whose data has been encrypted to roll back each file stored in the sync-and-share archive individually. Whereas endpoint backup enables a point-in-time restore of all files at once or a selective restore of the files an employee needs immediately.

> "Our previous, unstable backup situation has been thoroughly solved, thanks to Code42 CrashPlan. Now we have rock-solid endpoint data protection, a full admin console and complete, straightforward backup reports."

Tyler Smith, Executive IT Support, D+H Corporation

Product Features	Endpoint Backup	File Sync and Share
Protects all data on laptop or desktop	●	×
Backs up every version of every file	●	×
Backup happens automatically, continuously	●	×
Provides end-to-end encryption of data in-transit and at rest	●	●
Enables on-premises key escrow in any deployment	●	×
No user intervention required	●	×
Single administrator manages thousands of users via a single portal	●	●
Offers collaboration functionality	×	●
Allows access to files across platforms	●	●
Supports data migration	●	×
Supports mobile data access	●	●
Prevents data loss	●	×
Supports data privacy and compliance requirements	●	●
Supports e-Discovery/legal hold	●	●

Local deduplication is more secure, just as fast and better for recovery

If data security and recovery are your primary objectives, local deduplication is more secure and more reliable than global deduplication.

Backup vendors that promote global deduplication say it minimizes the amount of data that must be stored and provides faster upload speeds. What they don't say is how data security and recovery are sacrificed to achieve these "benefits."

Here's a key difference: with local deduplication, data redundancy is evaluated and removed on the endpoint before data is backed up. Files are stored in the cloud by the user and are easily located and restored to any device. With global deduplication, all data is sent to the cloud, but only one instance of a data block is stored.

They tell you: "You'll store less data!"

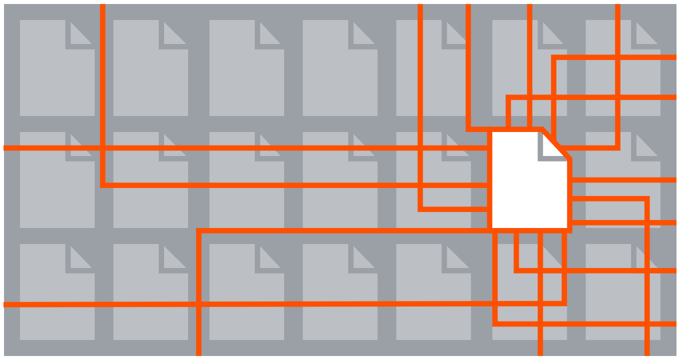
It's true that global deduplication reduces the number of files in your data store, but that's not always a good thing. Storing less data sounds like a benefit, especially if you're paying for endpoint backup based on data volume. But other than potential cost savings, how does storing less data actually benefit your organization?

For most organizations, the bulk of the files removed by the global deduplication process will be unstructured data such as documents, spreadsheets and presentations—files that are not typically big to begin with—making storage savings resulting from global dedupe minimal. The files that gobble up the bulk of your data storage are those that are unlikely to be floating around in duplicate—such as databases, video and design source files.

What they don't tell you: Storing less data doesn't actually benefit your organization. Smaller data stores benefit the solution provider. Data storage costs money and endpoint backup providers pay for huge amounts of data storage and bandwidth every month. By limiting the data stored to one copy of each unique file, the solution provider can get away with storing less data for all of its customers, resulting in smaller procurement costs each month—for them.

Vendors that offer global dedupe also fail to mention that it puts an organization at risk of losing data because (essentially) all the eggs are in one basket. When one file or data block is used by many users but saved just once, (e.g., the HR handbook for a global enterprise, sales pitch decks or customer contact lists) all users will experience the same file loss or corruption if the single instance of the file is corrupted in the cloud.

They claim global dedupe leads to faster uploads. Speed gains achieved by utilizing global deduplication are mostly undetectable. A quality endpoint backup solution will provide fast data uploads regardless of whether it uses global deduplication or local deduplication.



As the data set grows, global deduplication slows file restoration

What they don't tell you is global deduplication comes at a cost: restore speeds will be orders of magnitude slower than restoration of data that has been locally deduplicated.

With global deduplication, all of your data is stored in one place and only one copy of a unique file is stored in the cloud regardless of how many people save a copy. Rather than store multiples of the same file, endpoint backup that utilizes global deduplication maps each user to the single stored instance. As the data store grows in size, it becomes harder for the backup solution to quickly locate and restore a file mapped to a user in the giant data set.

Unique files or data blocks are indexed as they come into the data store and are not grouped by user. When the data store is small, it's relatively easy for the system to locate all of the data blocks mapped to one user when a restore is necessary. As the data store grows in size, the process of locating all of the data blocks takes longer. Global deduplication slows the restore process and forces the end user to wait at the most critical point in the process—when he or she needs to get files back in order to continue working.

Simplify your search for the right solution

Ready to adopt an enlightened data security strategy to protect your enterprise? You already know that endpoint data backup is the essential core, but how do you find the right solution? Here's what to look for:

1 Provides protection everywhere

Code42 CrashPlan provides centralized, cloud-based endpoint backup that works across geographies, platforms and devices. It's simple to manage, simple to scale and offers powerful features to solve other data collection, migration and security problems.

2 Protects end-user data across operating systems

The enterprise is not homogenous anymore. Apple devices set the standard in the consumer market, and executive and employee preferences for Apple devices have pushed Apple market share up in the enterprise. 92 percent of companies support Macs today.

Code42 CrashPlan backs up every file on Windows, Linux or OS X laptops and desktops—with a consistent experience across all platforms. It restores files to any computer or mobile device (including iOS, Android and Kindle Fire devices) any time, from anywhere, without requiring a VPN connection.

3 Simple, centralized end-user data control through the cloud

Code42 CrashPlan is a cloud-based SaaS backup that offers secure, non-stop protection for all end-user data on a centralized platform. When data is secured on a single platform, it enables self-service file recovery and data migration, data governance functions such as data retention rules, regulatory audits and compliance, and in-place legal hold.

4 Simplifies backup for IT from the moment it's deployed

Code42 CrashPlan provides complete control and visibility, granular administration, monitoring and reporting, and the ability to scale to many terabytes and many thousands of users—without adding IT headcount, headaches or in some cases, hardware.

5 Takes encryption and encryption key escrow very seriously

True data privacy means only the enterprise can view data content. Code42 CrashPlan deduplicates locally, encrypts data in transit and at rest, and enables the cloud customer to hold encryption keys in any cloud deployment. On-premises key escrow ensures that only the customer can view decrypted data—keeping it safe from the cloud vendor, government surveillance and blind subpoena.

6 Provides certain recovery from malware, ransomware, data loss, theft and breach

Breaches continue to increase—76 percent of organizations were breached in 2015 (2016 Cyberthreat Defense Report)—and endpoint devices are the weakest link in your security profile. Code42 CrashPlan ensures recovery of data—no matter the cause, without paying a ransom, without the original device, without the former employee. It's an investment in business continuity, risk mitigation and peace of mind.

7 Plugs the gap of human error—works where policies alone won't

Globally, 80 percent of companies said they were at risk from insider attacks. 55 percent said privileged users posed the biggest internal threat. And low security awareness among employees continues to be the greatest inhibitor to defending against cyber threats. Code42 CrashPlan gives IT the ability to plug these human-factor security gaps—to see who had what data when and where data was moved. Visibility of content helps IT address the risk of inadvertent and accidental leaks, exposure of sensitive data outside authorized channels and malicious insider theft.

8 Drives down data migration costs

The number one driver of data migration is technology refresh, followed by consolidation and relocation. While data migrations are routine, they pose known risks—including data loss and corruption, unexpected downtime, lease overruns and technical compatibility issues.

CrashPlan secures a copy of each file before tech refresh and OS migrations in a secure backup location—and makes it easy for end users to conduct their own data migration after the device has been imaged—cutting an IT task from hours to moments.

9 Accelerates and simplifies legal hold

Legal hold is expensive, disruptive and time consuming. Code42 CrashPlan leverages user backups to enable in-place legal holds and file collection without confiscating user devices. IT is able to offload the responsibility to legal personnel via a legal hold web app.

10 Supports rapid response to data incidents

InfoSec experts agree that data breaches are inevitable in today's enterprise world. A modern endpoint data backup solution provides 100 percent visibility and attribution of file content on any device, enabling IT to quickly identify a threat, mitigate the impact to reduce costs and determine if data on compromised devices (including lost or stolen devices) requires the organization to notify agencies or individuals of breach.

11 Helps your enterprise meet compliance requirements

The growing threats of data breach and cybercrime are driving new, heightened regulations in every industry. CrashPlan helps your enterprise meet evolving data privacy and compliance requirements—with features including flexible cloud options, robust security architecture, client-side encryption and real-time auditing and reporting—to minimize IT hassle and risk to the organization.

12 Offers cloud choices and the ability to select data destinations

Businesses and organizations are subject to unique data privacy, compliance and regulatory rules governing how and where data is stored, transmitted and controlled. CrashPlan enables businesses to comply with evolving regulations through data destination choices, data visibility and auditing features.

13 Supports complementary endpoint solutions

Endpoint backup is the core of an enlightened data security strategy, but it's not the only tool in the toolbox. CrashPlan works seamlessly with full disk encryption and file sync-and-share solutions—such as Box, One Drive and Dropbox—to create a complete data protection plan.

14 Designed for security-conscious enterprises

The enterprise is focused on data security and protection for good reasons. With the ability to hold up to 2TB of data on a single device, the power to do more is exponential and the risk of data loss is amplified. Most disaster recovery plans focus on data center servers and disk arrays; but almost two thirds of corporate data lives outside the data center on laptops, and 99 percent of employees have sensitive data on their laptop or desktop.

Subscription, cloud-based endpoint backup with CrashPlan offers secure, non-stop protection for all end-user data on a centralized platform. When data is secured on a single platform, it enables self-service file recovery and a wide variety of higher order data utilities to solve business, legal and security problems across the enterprise.

15 Future proofed for the mobile enterprise

Seventy percent of enterprise workforces will be mobile by 2020, making a scalable endpoint backup solution a necessity for modern enterprises. Only Code42 CrashPlan has built-in scalability with support for hundreds of thousands of concurrent users.

Data security starts on the endpoint

Modern enterprises make endpoint backup a critical element of their data security strategy because they value the data stored on endpoints.

Modern endpoint backup for IT

Code42 CrashPlan gives IT a comprehensive, single point of visibility and control across every end user in the enterprise—making it easier to overcome insider threat and recover from any type of data incident. Code42 CrashPlan is modern endpoint backup that takes IT off the hook for data migration by enabling end users to recover their own work—all the way to self-service data migration.

Modern endpoint back supports Information Security

The attack surface of the enterprise and the potential for breach and insider threat continue to grow. Code42 CrashPlan gives InfoSec visibility into data and data movement, so the enterprise can achieve full data attribution in response to breach. Code42 CrashPlan helps the enterprise meet risk, regulatory, and compliance requirements, and identify and monitor the source of data leakage.

Modern endpoint backup supports Legal teams

Code42 CrashPlan is the foundation for rapid, comprehensive legal hold administration. Its legal hold web app gives legal teams the ability to select custodians, apply rules and collect files during eDiscovery or regulatory audits—and reap time and cost savings.

MODERN ENDPOINT BACKUP

Protects against data loss
no matter the cause

Runs continuously
and automatically

Works on Windows,
Macs and Linux

Supports the mobile workforce
with no disruption

Helps you respond fast
to data incidents

Drives down
data migration costs

Drives down legal hold costs

Offers cloud choices

Lets you decide where
to store encryption keys

References:

1 http://bit.ly/1PrXubJ

2 http://bit.ly/1RhkaRB

3 http://bit.ly/1RysM28

4 http://bit.ly/1T6yvS3

5 http://bit.ly/1UNcO9K

6 http://ubm.io/1ZtOsm7

7 http://bit.ly/19Sp3xi

8 http://bit.ly/1hx7gtp

9 http://bit.ly/1RmiJjy

10 http://bit.ly/1UmaaJM

11 http://bit.ly/1UmaaJM

12 http://bloom.bg/1Rmulvr

13 http://intel.ly/1UaUl8d

14 http://bit.ly/1UmaaJM

15 http://bit.ly/1Si79WZ

16 http://bit.ly/1TGRpzM

17 http://bit.ly/1y7PFUj

18 http://onforb.es/1Mmwy2B

19 http://bit.ly/1WDU8ba

CONTACT CODE42 SALES
www.code42.com/contact

CODE42

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

Code42 is a global enterprise SaaS provider of endpoint data protection and security to more than 39,000 organizations, including the most recognized brands in business and education. Our highly secure cloud solutions enable IT and security teams to limit risk, meet data privacy regulations and recover from data loss, no matter the cause.