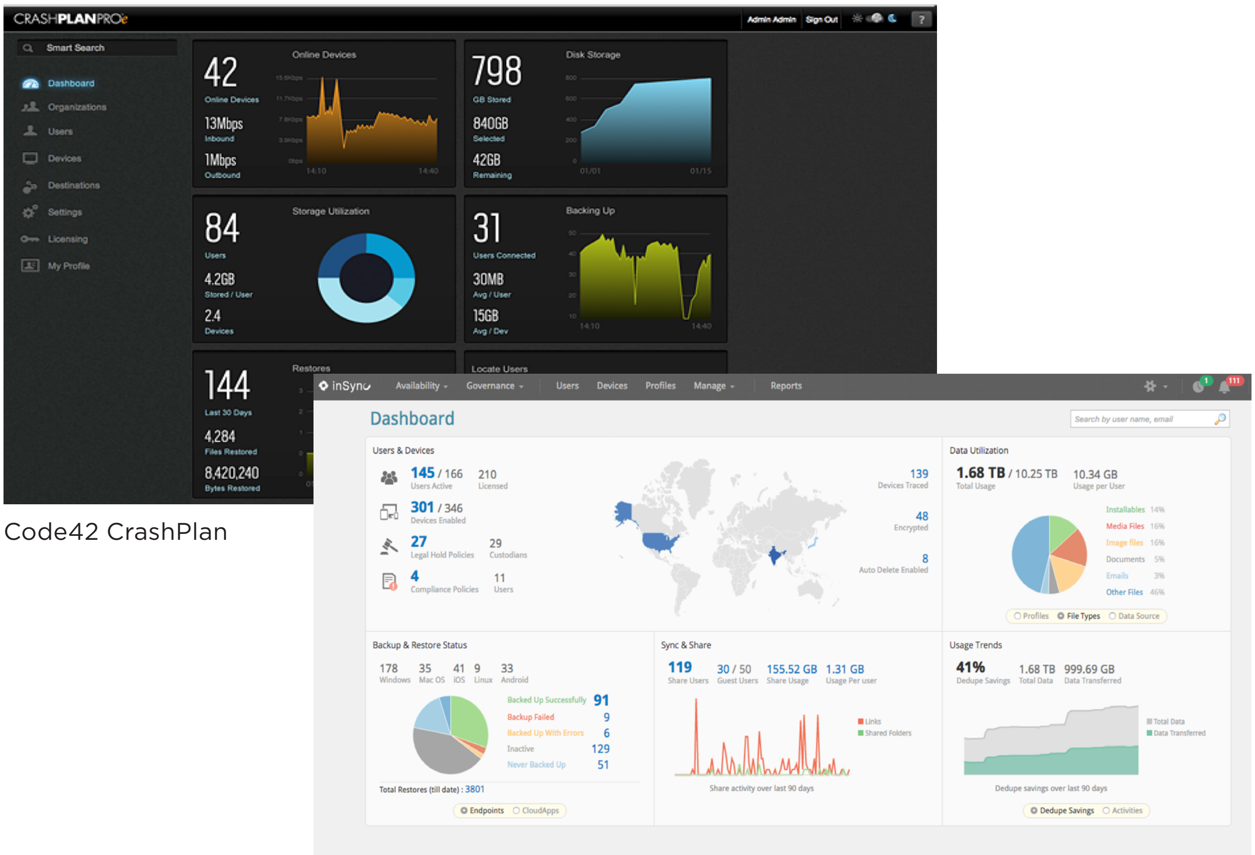
Druva inSync vs. Code42 CrashPlan



Code42 CrashPlan

Druva inSync

Table of Contents

Executive Summary

At first glance, Druva inSync and Code42 CrashPlan might seem similar, as both are designed for end-user data protection, provide flexible deployment options, license per-user and have some common features. However, inSync has several architectural advantages and integrated features, such as cloud application data collection & archival, proactive compliance, data loss prevention (DLP), file sharing, and data governance, which provide businesses with higher value at a lower total cost of ownership (TCO) than CrashPlan does.

Druva designed inSync as a unified end-user data protection, sharing, and governance solution that delivers the visibility and management needed for large enterprises. This approach enables organizations to benefit from the performance increases delivered by our unique global deduplication system, as well as minimize the data replication inherent with siloed solutions. Security and governance remain centralized, providing comprehensive audit trails, and the ability for legal hold across laptops, mobile devices, and cloud apps.

This report will compare the features of Code42 CrashPlan and Druva inSync across several different categories, including: data deduplication, device refresh & OS migration, legal hold & and eDiscovery, proactive compliance, security and data privacy, data availability and durability, and integrated file sync and share.

Why Switch from CrashPlan to inSync?

- inSync saves 80% in bandwidth and storage with global, application-aware, client-side deduplication.
- CrashPlan does not have the ability to globally deduplicate data across all users in an enterprise.
- CrashPlan’s dual-destination backups require twice the bandwidth as inSync.
- CrashPlan’s user profile backup for OS migration requires significant IT effort as well as limited support across device platforms.
- CrashPlan’s new legal hold capabilities are basic, using a classic backup model that requires IT/Legal to move the data to an intermediary preservation server. Moreover, CrashPlan’s legal hold capabilities allows Legal to customize the retention polices when creating a legal hold which violates Federal Rules of Civil Procedure (FRCP).
- CrashPlan does not backup mobile devices or containerize corporate data.
- CrashPlan’s datacenters are not ITAR, FISMA, ISAE3000, SOC-1 (SSAE 16/ISAE 3402) SOC-2 or SOC-3 certified.
- CrashPlan has no stated SLAs on data durability and availability.

- CrashPlan's security options trade-off enterprise level data accessibility for security and privacy, opening a hole for data loss through lock-out.
- CrashPlan does not offer mobile smart device remote wipe capability for DLP to prevent data breaches.
- CrashPlan does not offer integrated file sharing, requiring organizations to purchase a separate file sharing solution.

Features Comparison

Data Deduplication Techniques

Data Deduplication Techniques	Code42 CrashPlan for Enterprise	Druva inSync
Deduplication methodology	Variable-block level, only deduplicates across a single device	Object level, global across all user, and client-side
Application-aware deduplication	No	Yes
Email duplication	PSTs are evaluated as a single file	Deduplicates individual messages and attachments

CrashPlan

CrashPlan deduplicates only across data from a single device providing very limited bandwidth and storage savings.

- Variable-block based, byte level deduplication is not accurate at determining block boundaries (objects) to efficiently deduplicate objects within/across different file types
- The per-device model results in a single 100MB file, stored on 20 user's devices being backed up 20 times, whereas global deduplication which will only store it once.
- Without email awareness, a PST file must be assessed and backed-up every pass, resulting in a lot of wasted storage

inSync

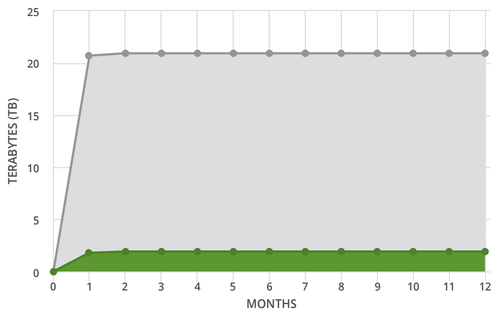
inSync's deduplication is global, application-aware, and client-side which results in 70-80% bandwidth and storage savings.

- inSync deduplicates data across all users/ devices in the enterprise
- Because of its application-aware nature, inSync provides optimal deduplication with Outlook, PDF, and Office files as it accurately determines block boundaries and can recognize objects within as well as across these file types
- inSync is far more efficient in backing up large PST files as it uses MAPI to deduplicate at the message/attachment level
- Bandwidth and storage savings mean less time spent in storage management, better end user experience, and lower TCO

Storage and bandwidth usage over time:

80% LESS

inSync will use 17 TB less storage and bandwidth (80% less) compared to traditional backup after 1 year of implementation.



Device Refresh & OS Migration

CrashPlan

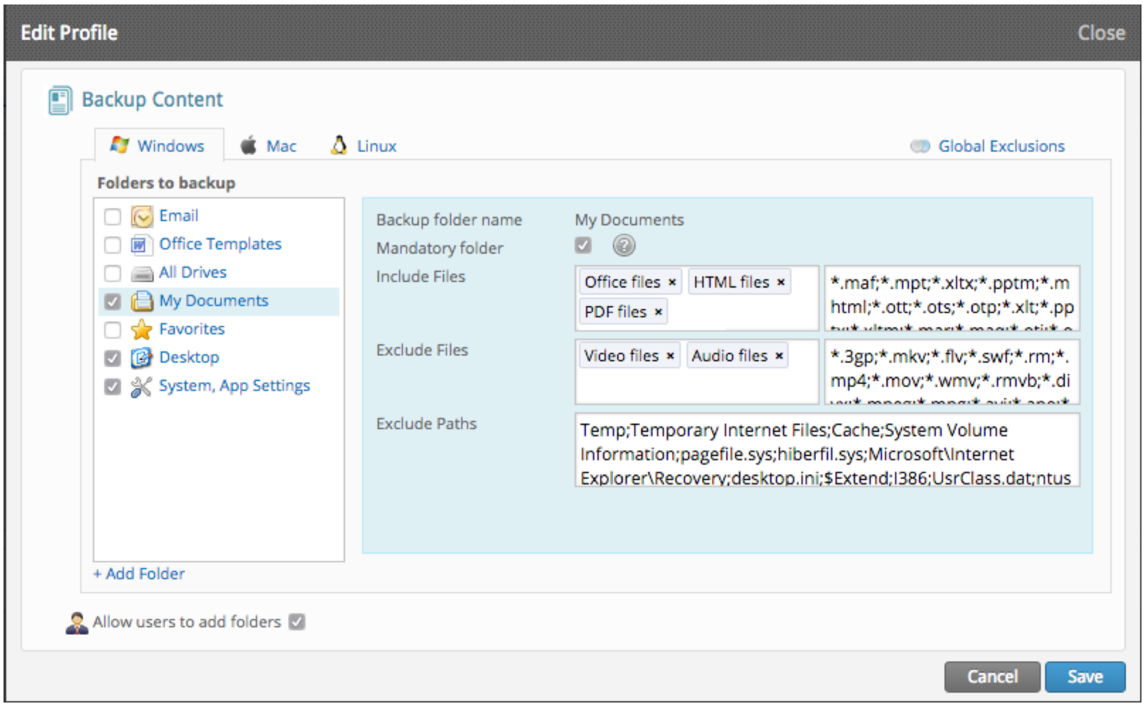
Currently CrashPlan only supports backing up of Windows user profiles, and does not support OS X environments.

CrashPlan uses Microsoft's User State Migration Tool (USMT) in migrating system settings and application data and requires .XML files to determine what is included in the profile backup. CrashPlan does not provide the default .XML files for USMT and requires users to supply/create them for profile backups
to occur.

For the CrashPlan app to backup user profile data, USMT must be installed or deployed on each device backing up to the Code42 server, requiring additional work for IT admins.

inSync

With inSync's Persona backup, users can backup system and application settings in addition to their files and folders.



Folders to backup

- ☐ Email
- ☐ Office Templates
- ☐ All Drives
- ☑ My Documents
- ☐ Favorites
- ☑ Desktop
- ☑ System, App Settings

Backup folder name: My Documents

Mandatory folder: ☑

Include Files: Office files × HTML files × PDF files × — *.maf;*.mpt;*.xltx;*.pptm;*.m html;*.ott;*.ots;*.otp;*.xlt;*.pp

Exclude Files: Video files × Audio files × — *.3gp;*.mkv;*.flv;*.swf;*.rm;*. mp4;*.mov;*.wmv;*.rmvb;*.di

Exclude Paths: Temp;Temporary Internet Files;Cache;System Volume Information;pagefile.sys;hiberfil.sys;Microsoft\Internet Explorer\Recovery;desktop.ini;$Extend;I386;UsrClass.dat;ntus

Allow users to add folders ☑

- Eliminates the need for painful bare metal restores (BMR) on endpoints
- Saves end-user time spent in manually reconfiguring system and application settings to get back their familiar working environment
- Can be used for OS migration or laptop refreshes, eliminating the need to purchase software specific to OS migration that has no use after the migration process is completed
- Makes replacement/refresh and OS upgrade/migration processes efficient with user self-restore of both data and settings

Legal Hold & eDiscovery

Legal Hold & eDiscovery	Code42 CrashPlan	Druva inSync
Federated search and legal hold	Limited	Yes
Chain of custody reports	No	Yes
Admin tamper-proof audit trails	No	Yes

Direct access for eDiscovery platforms	No	Yes (e.g. AccessData, Recommind, DISCO)
Cloud apps data collection & archival	No	Yes (Office 365, Google, Apps, Box, Salesforce)

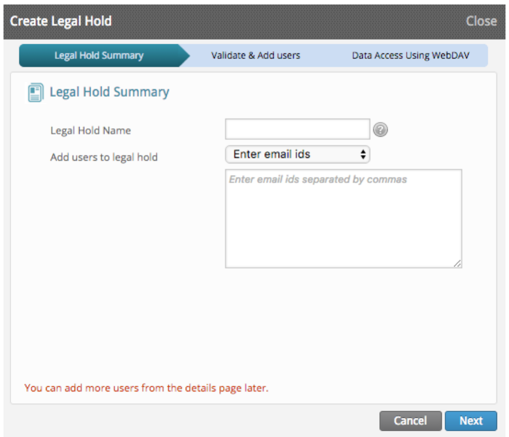
CrashPlan

Overall CrashPlan's legal hold capabilities are basic, using a classic backup model that requires IT/Legal to move the data to an intermediary preservation server. More advanced features such as full text search, investigative search and data culling, are notably absent from the product.

- CrashPlans legal hold web app allow Legal to customize the retention polices when creating a legal hold which violates Federal Rules of Civil Procedure (FRCP)
- No centralized access to data for a legal hold policy. IT or Legal needs to restore data for every user and users must restore files to a device (push restore).
- Because there is no centralized access to data for a legal hold this significantly increases the chances of spoilage and also does not retain metadata attributes for chain of custody reports
- No out-of-the-box connectors with any eDiscovery vendor
- No chain of custody reports
- Poor support for metadata attributes (Only support Creation date, Last modification date, Checksum, Full path, File size)
- Cannot scale for continuous investigations or cannot meet strict SLA's for quick data access for certain litigations

inSync

Druva inSync is the only endpoint data protection platform that delivers the needed capabilities to locate custodian data, place legal holds and provide an interface for eDiscovery ECA system ingestion.



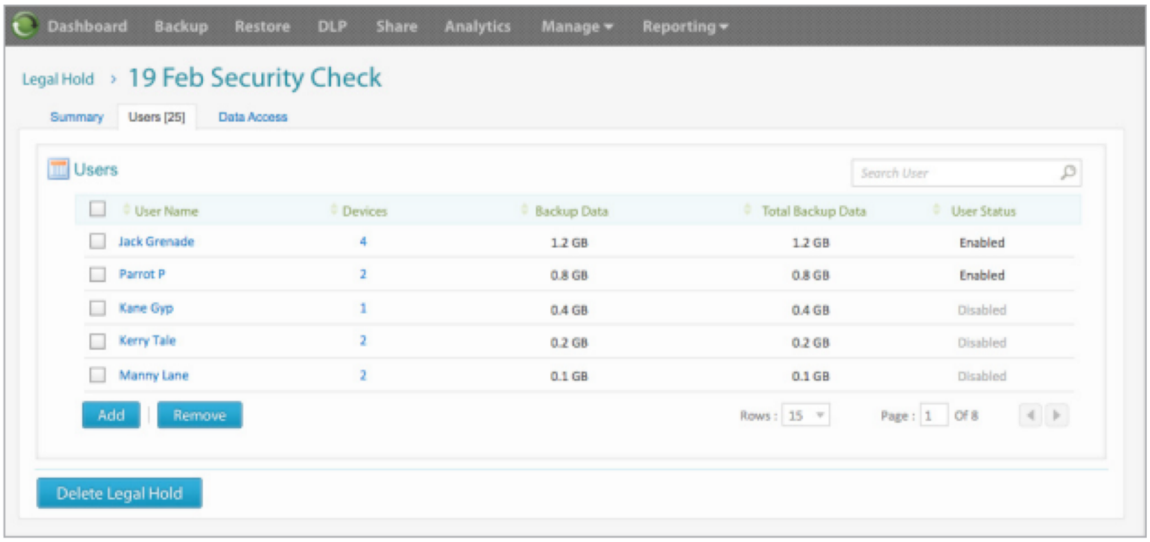
Legal Hold Summary

Legal Hold Name

Add users to legal hold: Enter email ids

Enter email ids separated by commas

You can add more users from the details page later.



□	User Name	Devices	Backup Data	Total Backup Data	User Status
□	Jack Grenade	4	1.2 GB	1.2 GB	Enabled
□	Parrot P	2	0.8 GB	0.8 GB	Enabled
□	Kane Gyp	1	0.4 GB	0.4 GB	Disabled
□	Kerry Tale	2	0.2 GB	0.2 GB	Disabled
□	Manny Lane	2	0.1 GB	0.1 GB	Disabled

- With centralized access to endpoint data, organizations can use inSync's federated search to identify the location of files — on which device they are stored, as well as the geographic location of the device itself.
- After identifying custodians via federated search or list import, organizations can place legal holds on stored data, suspending retention policies and preserving the content in place — ensuring it remains securely stored and immutable until it needs to be reviewed.
- inSync keeps full audit trails to the content that is stored and accessed within the system. These audit trails include all end-user and IT administrator activity and are tamper-proof to ensure proper information management procedures were followed.
- When legal is ready to transfer held data into an eDiscovery ECA system, inSync provides legal administrator access to review held data and expose it for ingestion over the network.

Proactive Compliance

Compliance	Code42 CrashPlan	Druva inSync
Ability to proactively track, monitor and be notified of potential data risks	No	Yes
Data capture across all devices	Limited to on-premises deployments	Yes

Cloud Apps Data Collection & Archival	No	Yes (Office 365, Google, Apps, Box, Salesforce)
Predefined compliance regulation templates	No	Yes (ex. HIPAA, GLBA, PCI)
Data capture across cloud applications	No	Yes (Office 365, Google, Apps, Box, Salesforce)
Ability to search across all devices	Ability to search across a single user only	Yes

CrashPlan

Code42’s endpoint monitoring uses the CrashPlan app to identify different types of security events on each device and is simply a data monitoring/logging tool, that lets admins know of security events. Code42’s endpoint monitoring requires integration with Splunk Enterprise for any advanced visibility or insights.

CrashPlan's pattern matching feature relies on a rule-based framework called YARA, which requires admins to place a file on each end-user’s device that uses endpoint detection. CrashPlan's pattern matching feature also requires the custom scripting and maintaining of the YARA rule file for every pattern a admin wants to identify. Moreover YARA rules are incapable of reading PDFs, servilely limiting what is captured.

inSync

With inSync’s proactive compliance, enterprises can automate finding data risks either related to industry regulations (such as HIPAA, PCI DSS, or GLBA) or based on their own criteria (human resources, intellectual property,financial policies) stored across end-user devices and cloud applications.

- Centralized compliance dashboard: Compliance, security, and legal teams can access an easily-navigable dashboard that permits authorized users to visualize corporate data by data source, compliance risk type, risk level, user types, and other pertinent information.
- Predefined, customizable compliance templates: Organizations can select from predefined compliance templates or customize their own. Proactive Compliance automatically scans the data -- wherever it is -- and highlights troublesome items (such as social security numbers or health record data), and alerts the right people when suspect materials are found.

- Investigative search: When handling an investigation request by the legal team, authorized users can use inSync's deep-search and legal hold capabilities to locate suspect materials, identify possible custodians, and place data on hold for eDiscovery purposes.

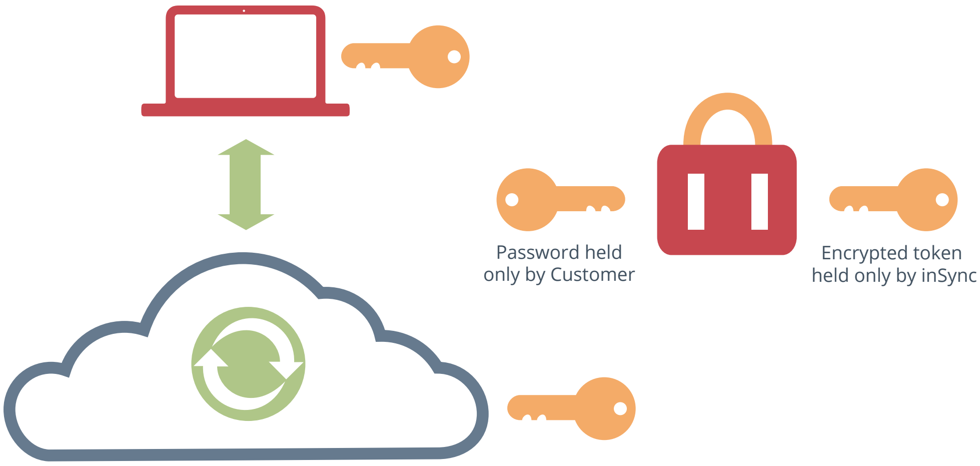
Security and Data Privacy

Security and Data Privacy	Code42 CrashPlan	Druva inSync
Encryption in transit	128-bit AES (default)	256-bit TLS
Encryption at-rest	256-bit AES	256-bit AES
Data encryption on endpoints	No	Yes
Certified cloud infrastructure	Yes	Yes
Digital envelope encryption key management	No	Yes
Native end-user app	No, Java based	Yes

CrashPlan

CrashPlan provides incomplete data security, and its data privacy measures leave corporate data at risk of exposure.

- CrashPlan stores encryption keys on end user devices in plain text


Password held only by Customer
Encrypted token held only by inSync

- CrashPlan's most basic security leaves it open to cloud data privacy issues, whereas their stronger encryption choices prevent compliance and legal teams from accessing employee stored files for auditing and litigation
- Because CashPlan still uses Java Virtual Machine (JVM), as the number of users and devices in a Code42 environment increases, the amount of Java Virtual Machine (JVM) heap space memory consumed in Code42 server(s) will also increase, resulting in Java "out of memory" (OOM) errors

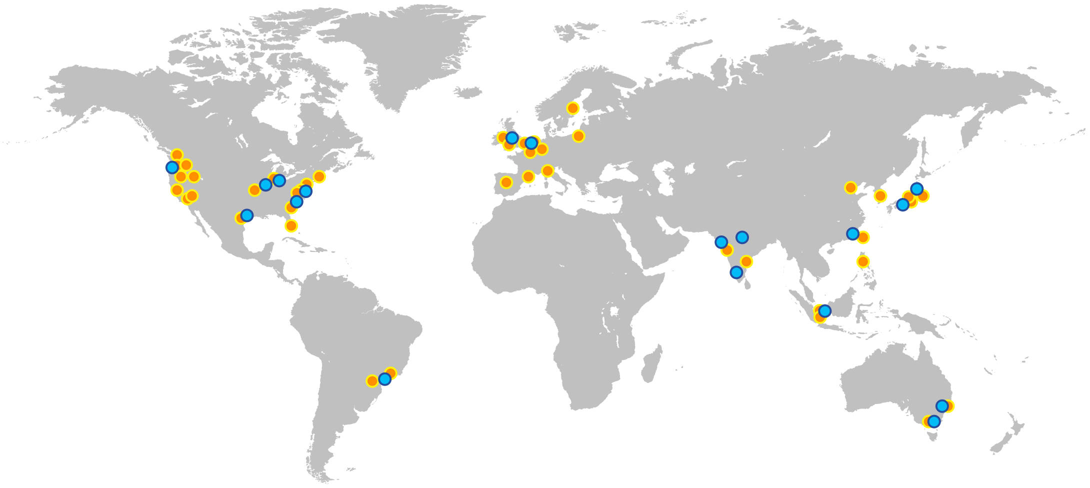
inSync

With inSync, customers have complete data privacy.

- Unique digital envelope encryption ensures that encryption keys are never stored in the cloud or on endpoints, preventing anyone except the customer from accessing data
- inSync Cloud customers can easily comply with data residency laws given access to multiple regions

Availability and Data Durability

Industry's best cloud infrastructure



amazon web services

Microsoft Azure

Certified cloud operations

Amazon Web Services Certifications

Certified Cloud Operations

CrashPlan

CrashPlan's cloud does not replicate data and has no stated SLAs.

- No data redundancy across Code42 data centers
- CrashPlan's disaster recovery plan requires dual destination backups that increase storage/ bandwidth & costs

inSync

Druva is built on native cloud technologies utilizing the power of the public cloud - Amazon Web Services (S3, DynamoDB, EC2), and Microsoft Azure, the two highest rated and most secure infrastructures available. By taking this approach we've removed all bottlenecks to scalability and elasticity that tends to plague systems that were initially designed for on-premise and retrofitted to the cloud. Our customers can leverage any of the AWS or Azure regions, and many of our global customers use multiple regions for addressing data residency/privacy regulations; for example in Germany.

Integrated file sync & share

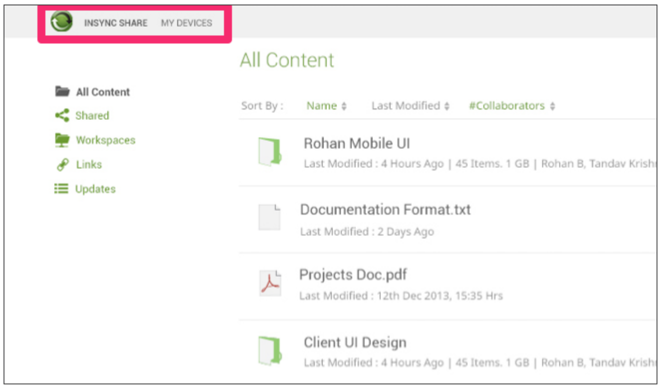
Integrated File Sync & Share	Code42 CrashPlan	Druva inSync
Integrated file sharing with IT visibility	No	Yes, integrated

CrashPlan

Code42 announced the end of life for SharePlan, in August 2015.

inSync

inSync was the first provider to integrate secure file synchronization and sharing with endpoint backup, and seamlessly integrate user productivity while giving IT admins granular control over sharing.



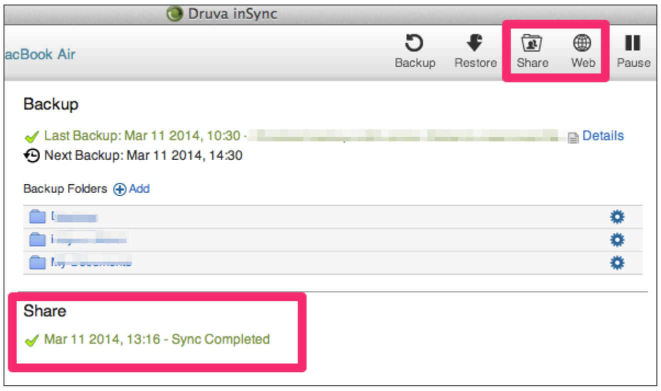
Rohan Mobile UI
Last Modified : 4 Hours Ago | 45 Items. 1 GB | Rohan B, Tandav Krish

Documentation Format.txt
Last Modified : 2 Days Ago

Projects Doc.pdf
Last Modified : 12th Dec 2013, 15:35 Hrs

Client UI Design
Last Modified : 4 Hours Ago | 45 Items. 1 GB | Rohan B, Tandav Krish

- File sharing data is globally deduplicated with backup data which amplifies bandwidth & storage savings
- Deep IT control & visibility
  - → enable sharing, share with who, mobile sharing, external/ link sharing
  - → user activity streams
- Integrated document viewer (view only links, expire link by # of views)
- Selective sync (save bandwidth, disc space on endpoint)



✓ Last Backup: Mar 11 2014, 10:30 - [redacted]
Next Backup: Mar 11 2014, 14:30

[redacted]

✓ Mar 11 2014, 13:16 - Sync Completed

Conclusion

Code42 CrashPlan is an inadequate backup solution for the needs of today's mobile enterprise. On the other hand, inSync offers the industry's best data protection solution for all enterprise endpoints: laptops, smartphones and tablets. Validated by leading analysts firms (Gartner rated Druva highest overall product score three time in a row) and a growing customer base, inSync dramatically improves IT efficiencies and end-user productivity. A recent study conducted by the Ponemon Institute, Quantifying the Value of Unified Endpoint Data Management, indicates that enterprises can save more than $8,100 per user by employing a solution like inSync, which integrates endpoint backup with secure file sharing, DLP and analytics.

Index: Product Comparison Chart

	Code42 CrashPlan	Druva inSync
Cloud Infrastructure		
Data redundancy across multiple data centers	Not available	Yes, can sustain concurrent loss of data in two facilities (Cloud)
Certifications	SAS 70 only	SOC-1 (SSAE 16, ISAE 3402 (formerly SAS 70), SOC-2, SOC-3, ISO 27001, PCI DSS Level 1 (Cloud)
Availability and Data Durability	Not advertised	99.95% Availability, 99.99999% Data Durability (Cloud)
Cloud Architecture	No, private cloud in a public cloud data center	Yes, native cloud architecture with elastic provisioning
Performance		
Global Data Deduplication	Dedupes only data from same device, resulting in backups of much larger data sets that take longer, consume more bandwidth and storage, and are intrusive to the end user	Global/enterprise-wide, reduces data redundancy across all users/devices to provide the best performance in storage and bandwidth savings
Dedupe Granularity	Block-based, incapable of recognizing file formats, objects within files, and across different file types, resulting in poor bandwidth/storage savings	App-aware, object-level, able to understand different file formats and intelligently deduplicate objects within and across different file formats, providing dramatic bandwidth and storage savings
WAN Optimization	Not available	Yes, optimizes packet size and number of threads depending on network noise and latency, making best use of available bandwidth
Bandwidth Throttling	Sub-optimal maximum bandwidth cap	Based on percentage of available bandwidth (optimal for modern workforce connecting over multiple networks)
CPU Throttling	Available	Available

Data Capture Frequency	CDP (minutes)	CDP (minutes)
Security		
Network Encryption (data encryption in transit)	128-bit AES	256-bit SSL
Storage Encryption (data encryption at rest)	256-bit AES	256-bit AES
SSO	Not available on mobile devices	Available on all devices
Encryption Key Management	Overhead of maintaining Master Server on-premise	Digital envelope encryption provides complete security and data privacy with no hardware required on-premise
Encryption Key Stored on Client Device	Yes, in plain text	No
On-device Data Encryption	Not available	Yes
Remote Wipe Capability	Not available	Yes
Native end-user app	No, Java based	Yes
Administrator Experience		
Central Management Console	Yes	Yes
Mass Deployment	Needs custom scripting	In product tools, no custom scripting required
Legal Hold & eDiscovery		
Federated search and legal hold	Limited	Yes
Chain of custody reports	No	Yes
Admin tamper-proof audit trails	No	Yes
Direct access for eDiscovery platforms	No	Yes (e.g. AccessData, Recommind, DISCO)
Cloud apps data collection & archival	No	Yes (Office 365, Google, Apps, Box, Salesforce)

Compliance		
Ability to proactively track, monitor and be notified of potential data risks	No	Yes
Data capture across all devices	Limited to on-premises deployments	Yes
Cloud Apps Data Collection & Archival	No	Yes (Office 365, Google, Apps, Box, Salesforce)
Predefined compliance regulation templates	No	Yes (ex. HIPAA, GLBA, PCI)
Data capture across cloud applications	No	Yes (Office 365, Google, Apps, Box, Salesforce)
Ability to search across all devices	Ability to search across a single user only	Yes
Supported PC/ Laptop Platforms	Windows/Linux/Mac	Windows/Linux/Mac
Smartphone/Tablet Backup	Not available	iOS and Android
Mobile Access	iOS, Android, Win Mobile 8	iOS, Android, Win Mobile 8
Content Variety		
Files/Folders	Yes	Yes
Email Archives	Not efficient with PST files	Yes. App-aware technology uses MAPI for optimal PST backup
System and Application Settings	Limited, requires custom .XML scripts and no support for Mac	Yes, backup of user system and application settings simplifies OS migration and laptop replacement
Beyond Backup		
Data Loss Prevention	Not available	Yes, includes data encryption on endpoints, remote wipe and geo-tracking
Integrated File Sharing with IT Visibility	No	Yes
Advanced Data Insights	Not available	Yes

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information - dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at http://www.druva.com and join the conversation at twitter.com/druvainc.

The information contained in this document is subject to change without notice. Druva Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the performance, or use of this manual.

Q117-CON-10581

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com