druva

Evaluation Guide

Druva inSync versus HP Connected Backup
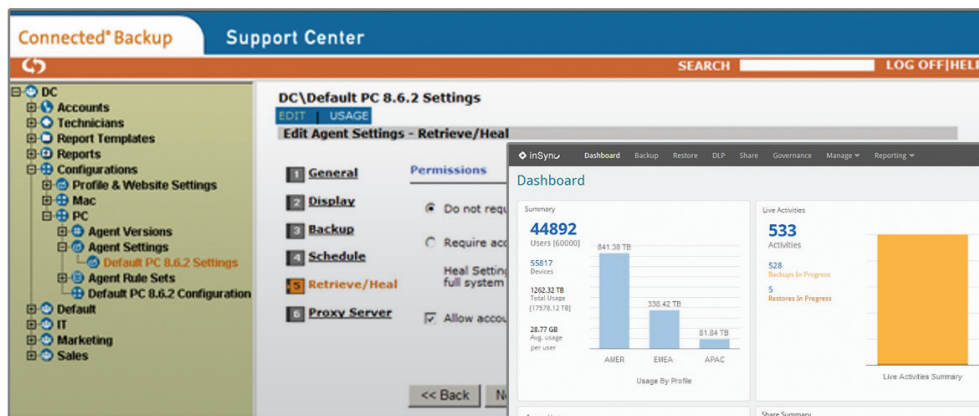
hp Connected

inSync

Table of Contents

Executive Summary

This evaluation guide is designed for IT professionals looking for a modern approach to endpoint backup, and for an alternative to HP Connected Backup. The information provided in this guide is based on feedback from customers who have switched from HP Connected to Druva inSync.

Traditional endpoint backup such as HP Connected Backup was designed to backup data on desktop computers. With the rise of mobile computing, this legacy solution was subsequently adapted to handle backup for endpoints (laptops, smartphones, and tablets). As a result, legacy solutions like HP Connected Backup offer limited support for efficient data deduplication, data transfer over variable bandwidths, and backup across varied types of mobile devices. In addition, HP Connected Backup offers only basic security features, and its IT interface requires significant effort to install, deploy, and maintain.

In contrast, Druva inSync was designed for today's dispersed data environment brought about by the rise of the mobile workforce. Designed to protect and govern data on endpoint devices, Druva inSync features advanced deduplication, eDiscovery enablement, WAN optimization, full mobile data backup, and data loss prevention. Centralized management with integrated mass deployment makes installing and managing inSync simple for IT.

The overview below compares the features of Druva inSync with HP Connected Backup across several key categories, including: data deduplication, mobility and BYOD, installation and management, performance and end user experience, and security.

Common Enterprise Concerns with HP Connected Backup

- A common issue with HP Connected Backup is its slow and intrusive operation. Due to the less than optimal impact on end user productivity, users often turn off backups, leaving data unprotected.

- HP Connected Backup does not protect against data breach for lost or stolen endpoints.

- HP Connected Backup is licensed per device; it does not support the notion of multi-device ownership or multiple devices being backed up by a single user.

- HP Connected Backup has minimal support for mobility or BYOD, with data access for a limited number of operating systems and device types.

- A common customer complaint is that HP Connected Backup is difficult to install and deploy, and requires significant IT effort to manage.

- HP Connected Backup requires significant bandwidth and storage, adding to its high TCO.

- HP Connected Backup does not continually protect data; it only offers daily backups.

- HP Connected Backup cannot enable efficient OS migration or laptop refreshes as it does not back up system data and application settings.

Feature Comparison

Data Deduplication

The quality of data deduplication in an endpoint backup solution can significantly impact end-user productivity, data availability, and overall costs.

Data Deduplication Technique	HP Connected Backup	Druva inSync
Global deduplication	File level	Object level
Application-aware deduplication	No	Yes
Email deduplication	Attachments only	Messages and attachments

HP Connected Backup

HP Connected Backup offers basic block-level deduplication, resulting in minimal reduction of the volume of backup data. This has a limited impact on bandwidth and storage, resulting in backup processes that are large and slow.

- Delta Block® deduplicates at the file level.
- SendOnce® eliminates duplicate files across user archives.
- Optional, PC-only email optimization deduplicates attachments only.

Druva inSync

Druva inSync employs global, client-side, application-aware deduplication technology, resulting in backups that require 80% less bandwidth and storage than do other solutions -- particularly when compared to HP Connected Backup.

- Deduplicates data at the object level (sub-file level).
- Deduplicates data across all users and their devices.
- Deduplicates data at the client side, which reduces bandwidth requirements.
- Application-aware deduplication eliminates duplication of objects within and across file types by taking into account the on-disk formats used by commonly-used applications (Outlook, Microsoft Office, PDF).
- Deduplicates Outlook data by using its MAPI interface to identify message folders and determine newly added, changed, or deleted messages.
- HyperCache, Druva inSync's server-side selective in-memory cache, reduces disk I/O by up to 90%. That gives significant wins in scalability.

Data Governance

Endpoint backup solutions do more than simply back up data. They also can enable litigation readiness to extend the value of your data protection strategy.

Visibility and Control Over End-User Data	HP Connected Backup	Druva inSync
Data loss prevention	No	Yes
Cloud applications	No	Microsoft Office 365 (Box, Google Drive coming soon)
eDiscovery enablement	No	Yes
Proactive compliance	No	Yes

HP Connected Backup

- No integrated legal hold or eDiscovery enablement.

- Separate eDiscovery solution needed.

- No administrative or user audit trails.

- No data loss prevention capabilities, resulting in high economic impact when a device is lost or stolen.

Druva inSync

Druva inSync combines user data across laptops, mobile, and cloud applications (beginning with Office 365) to provide centralized visibility, full-text search, and management to meet enterprise data governance needs. From a single, unified dashboard, IT easily can create data policies, automate compliance monitoring, administer legal holds and provide access for eDiscovery — all without impacting employee productivity in the smallest way.

- Federated, full-text search enables administrators to locate data in any file across all users, devices, and storage locations. This makes it easier to find information for compliance and legal needs.

- Automated monitoring searches across end-user data sources; it alerts stakeholders of potential risks from the use or distribution of sensitive data (e.g. Protected health information (PHI), Personally identifiable information (PII), Payment card industry (PCI)).

- Preconfigured compliance templates provide pre-built configurations for the most common data regulations.

- Built-in legal hold workflow facilitates the collection and preservation of relevant custodian data for legal teams while maintaining employee productivity.

- Remote wipe of data stored on lost or stolen devices can prevent expensive data breaches.

Mobility and BYOD Support

Given the rise in the number of mobile employees and the amount of data stored beyond the corporate firewall, support for mobile devices and workflows is critical in any endpoint backup solution.

| Mobility and BYOD Support	HP Connected Backup	Druva inSync
Multi-device ownership	No, licensed per device	Yes
Mobile apps	Tablets only	Smartphones and tablets
Self-deploy and self-restore	Self-restore only	Yes
Data backup for smartphones and tablets	No	Yes

HP Connected Backup

HP Connected Backup has minimal support for mobility or BYOD. Data access works only with a limited number of operating systems and device types.

- HP Connected Backup backs up only Windows and Mac laptops. Linux users are out of luck.

- Mobile apps are available only for Apple iPad and Android tablets.

- HP Connected Backup is licensed per device. It does not support the notion of multi-device ownership or multiple devices backed up by a single user. In addition to costing more per user (since each device has to paid-for separately), it means more management complexity, because IT has to track which users own which devices. (Just what you needed: More work!)
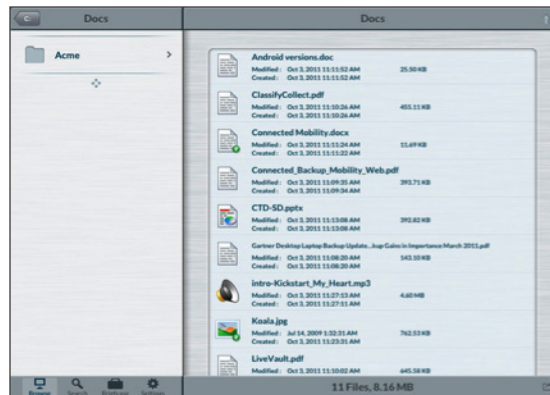

Connected iPad application is for access only and does not protect data on tablets.

- HP Connected Backup's tablet apps provide end-users with access only (that is, you can look at the data stored elsewhere). The tablet software does not backup corporate data or protect data on the device with mobile data loss prevention (DLP).
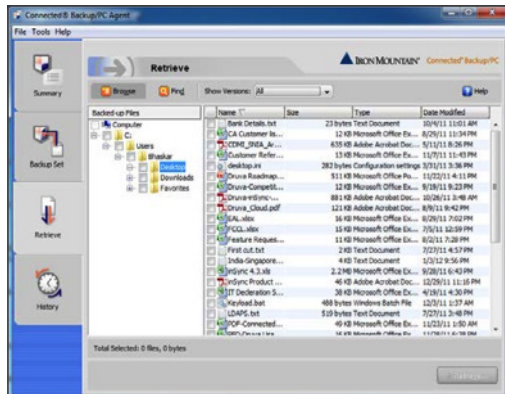
Connected client allows restores only from a single device
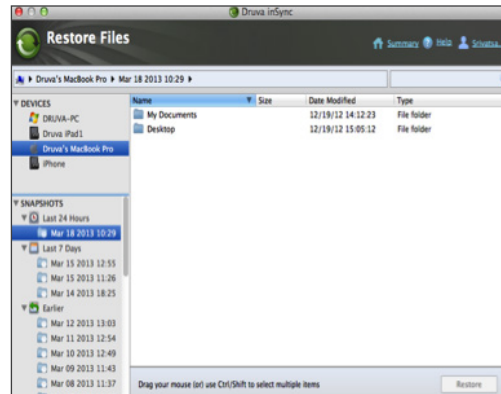
inSync provides a multi-device view for access and restore

- HP Connected Backup must be deployed by IT. It cannot be self-deployed by users. (More work for the IT department!)
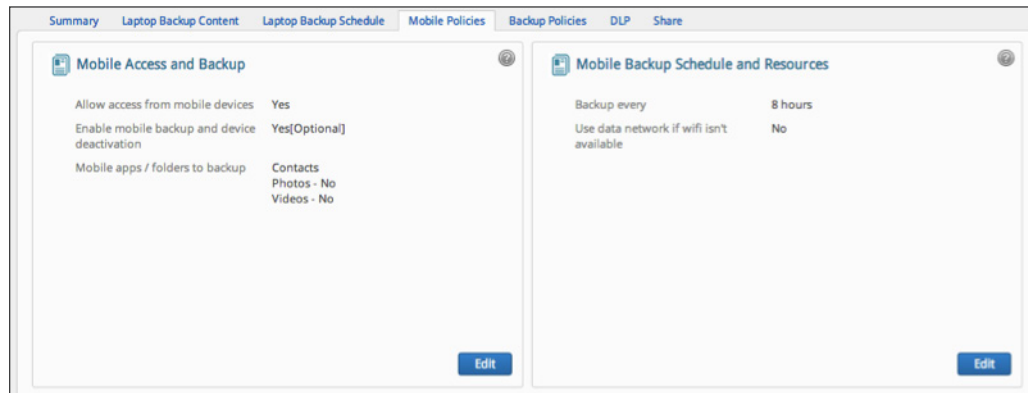
Druva inSync

- Druva inSync covers a broad variety of OS and device platforms including Windows, Mac, Linux, Apple iOS, Android, and Windows 8 mobile.

- Druva inSync has a single license per user, for any number of devices.

- Users can self-deploy and self-restore their devices. IT can set up policies to limit access or otherwise make sure the user gets what she needs (and not the things to which she should not have access), but certainly the user does not require IT intervention. This makes users happier, and prevents IT help desks from having to answer 2:00am phone calls. Result: Less crankiness all around.

- Users can access and restore data backed up from any device using the client, inSync Web, or the mobile app. It's their data, wherever it happens to reside.
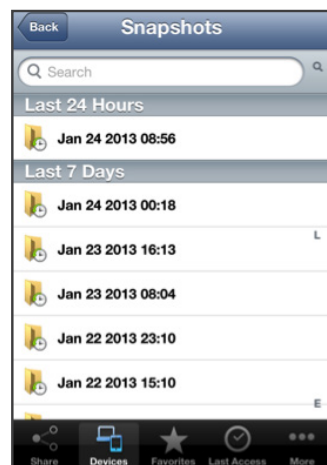
Device and snapshot views of the inSync iPhone Application

- The Druva inSync mobile app backs up corporate data for both corporate and BYOD smartphones and tablets.

- Data loss prevention capabilities allow corporate data to be remotely wiped from devices. That is: When a user leaves his phone on the plane, inSync can delete the company data (and optionally other information, such as those adorable cat photos; or everything on the device) from the phone. Then the only expense is buying a new phone (which can be provisioned with the always-backed-up data), and the business doesn't have to worry about the data getting into the wrong hands.

- File sharing lets users securely collaborate while providing IT visibility and control over corporate data.

inSync Mobile Policies

- Druva inSync's BYOD-related policies allow IT administrators the flexibility to manage user-owned devices. In other words: It's all under IT's control, so while you can give users power, you don't have to depend on them having a clue. Among those policies, for example, is the ability to enable mobile device access and mobile sharing based on a user profile, or to limit where certain actions can be done (such as permitting mobile backup only over Wi-Fi networks).

Deployment, Installation, and Management

The ease and speed of deployment of an endpoint backup solution can reduce overall costs and enable more efficient use of limited IT resources.

Installation and Management	HP Connected Backup	Druva inSync
Silent deployment	Yes	Yes
No custom scripting required	Requires custom scripts	Yes
Installation time	Days	Minutes
1-click configuration	No	Yes
Centralized administration	Yes	Yes

Connected Administrator Console

inSync Administrator Console

HP Connected Backup

HP Connected Backup requires significant IT time and effort to install and maintain.

- Mass deployments require IT to write custom scripts.
- HP Connected Backup requires installation of several Connected Data Center servers (registration server, backup server, Web server), Support Center, Account Management Website, and Connected Backup databases. That's a lot to manage.
- Admins must set up communities and accounts, create agent configurations, and set up complex rule sets with file inclusions and exclusions before backups and restores can be initiated.
- HP Connected Backup's Support Center interface is inefficient for administration and management of a large number of users and devices.

Druva inSync

inSync features integrated tools, pre-configured options, and a visual interface for simple installation and maintenance.

- With its in-built mass deployment tools, inSync does not require custom scripts to be written. Druva inSync's integrated mass deployment relies on Active Directory, Microsoft CCM, and Casper (JAMF software) -- tools that administrators already know -- to deploy Druva inSync clients without user involvement.
- Druva inSync can be set up on-premise in a matter of minutes.
- Preconfigured user-profiles can be easily extended to create new ones, so administrators can roll ot new user types without breaking a sweat.
- One-click quick configuration allows administrators to set up commonly-used data sources for backup, such as email, desktop, and documents.
- A centralized administrative console gives administrators seamless management of users, policies, and data across inSync storage nodes. The same set of profiles and policies can be applied across endpoint backup, file-sharing, and DLP.
- Global real-time federated search helps administrators to quickly locate a specific file on any endpoint.
- Reports and data analytics give everyone a view from a height or in great detail with out-of-the-box report filters: detailed information on users, devices, files, versions (restore points), date modified, and size.
- Watch the watcher: View administrator activities with an undeletable stream of all activities including managing users, data, storage, and reports.

Performance

How your endpoint backup solution handles variable bandwidths and environments impacts end-user productivity as well as the reliability and integrity of your data backups.

| End-user Experience	HP Connected Backup	Druva inSync
Bandwidth caps	Yes	Yes
Percentage-based bandwidth throttling	No, only maximum bandwidth caps	Yes
CPU throttling	No	Yes
WAN optimization	No	Yes

HP Connected Backup

HP Connected Backup has limited bandwidth-throttling options and data-reduction techniques. Because the backup demands so much system attention, backups are intrusive for users. That motivates them to turn off the client, leaving data unprotected.

- HP Connected Backup offers only maximum bandwidth caps.

- Its over-simplistic deduplication techniques have minimal impact on bandwidth and storage. So the software consumes system and network resources, and uses far more storage than it ought.

Druva inSync

Druva inSync has multiple bandwidth throttling options and advanced deduplication techniques. Backups take place in the background -- as they should -- without bothering users in the least; data remains continuously protected.

- Druva inSync dynamically throttles bandwidth during backups with percentage-based bandwidth throttling. Administrators (and users, if enabled) can specify bandwidth usage as a percentage of what is available.

- Druva inSync also offers maximum and minimum bandwidth caps.

- With Druva inSync's CPU throttling, CPU priority can be assigned so that backups do not interfere with users' high-priority applications. (If you need to get that project done on Friday afternoon, the last thing you want is the backup utility grabbing all the computer's attention.)

- The WAN optimization engine analyzes available network resources, selects the appropriate packet size, and spawns multiple threads to make the best use of the available bandwidth. Interrupted backups and restores are automatically resumed.

- Advanced deduplication at the client-side minimizes bandwidth and storage requirements for smaller, faster backups.
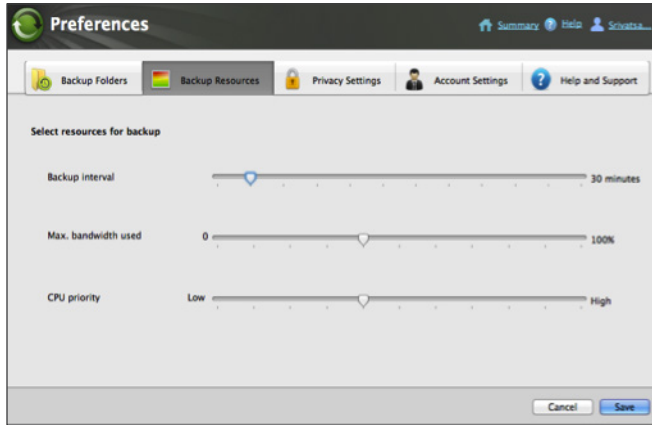
inSync bandwidth and CPU throttling from the client
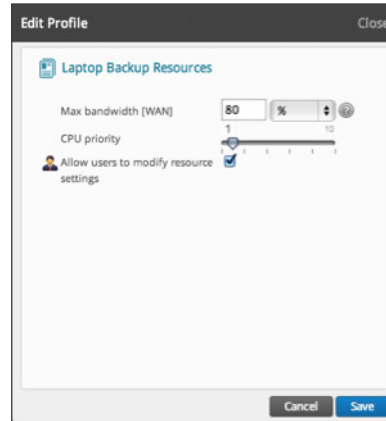
inSync bandwidth & CPU throttling from the admin console

Data Protection

Backup solutions should enable continuous and seamless backup and restores for protecting critical business data wherever it resides.

Data Protection	HP Connected Backup	Druva inSync
Manual and automatic backups	Yes	Yes
Continuous data protection	Daily	Minutes
System and application settings backup	No	Yes
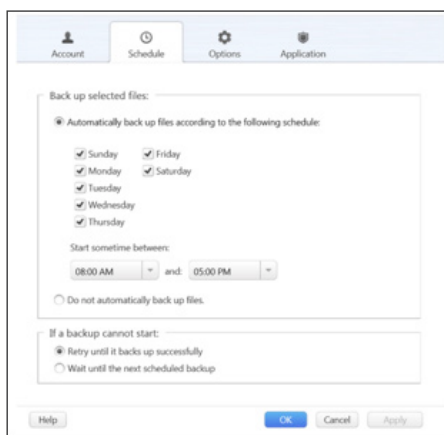
Connected Backup Scheduling
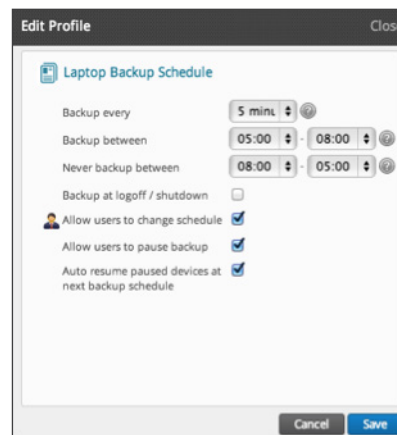
inSync Backup Scheduling

HP Connected Backup

HP Connected Backup allows manual backups or automatic backups at a daily frequency. HP Connected Backup backs up data only and does not backup any personal settings.

Druva inSync

inSync gives you continuous and non-intrusive data protection, not just daily snapshots. It can be configured to backup changes within minutes of their occurrence, without interfering with end-user productivity. If even that isn't often enough, inSync allows end users and administrators to initiate manual backups at any time.

inSync is the only endpoint backup solution to backup personal settings as well as data. With inSync's Persona Backup, which goes beyond backing up only user data, users can get right back to work in their familiar environment, saving them extensive time re-configuring device settings.

- inSync eliminates the need for time- and resource-intensive bare metal restores on laptops. This saves end users time spent in manually reconfiguring settings to get back their familiar working environment. (Give me my favorite desktop background! And re-set my schedule notification defaults the way I want them!)

- inSync enables efficient OS migrations and laptop refreshes with self-service restore of data, as well as system and application settings.

IT-Managed File Sync and Share

Gives IT teams control and visibility over business data, while also appealing to the user needs of simple and easy access.
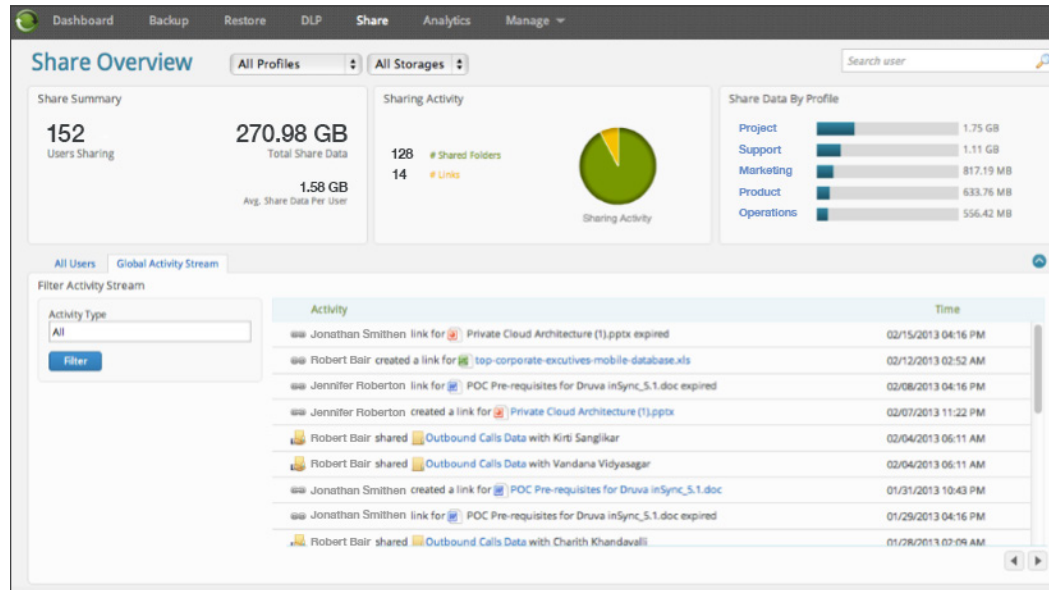
HP Connected Backup

HP Connected Backup does not offer integrated file sharing, requiring organizations to purchase a separate file sharing solution.

Druva inSync

inSync integrates endpoint backup with enterprise-ready file sharing. This gives IT visibility and control, and employees can collaborate on file collections without having to break IT's data sharing policies. Plus they get ease-of-use and a single-client experience.

- Users can selectively sync shared folders to their devices or simply view shared folders on the inSync Web client.

- Mobile sharing works with iOS, Android, and Windows 8 Mobile.

- Files can be shared with external collaborators via automatically expiring links, to prevent outsiders from access to data long after they need it.

- To further control access to corporate data, view-only links display files in-browser using Druva inSync's document viewer, and thus prevent downloads.

- Policy management allows IT to configure sharing permissions within and outside the organization, enable sharing on mobile device, and setting data-retention policies.

- Real-time user activity streams shed light on sharing patterns within the enterprise and offer visibility into the location of sensitive corporate data.

- IT has full visibility into all sharing activities.

inSync Admin Console File Sharing

Conclusion

A distributed workforce provides real challenges in enterprise scalability and IT efficiency. Legacy end-point backup solutions such as HP Connected Backup were not created to reflect the reality of a changing mobility landscape.

On the other hand, Druva inSync offers the industry's best end user data protection solution for enterprises, whether the data resides on a device or in the cloud. Validated by leading analysts and with a rapidly growing customer base, inSync dramatically improves IT efficiencies and end-user productivity, while enabling enterprises to address data governance challenges of users' dispersed data.

Comparison Summary

Feature	HP Connected Backup	Druva inSync
Data Deduplication Techniques		
Global deduplication	File level	Object level
Application-aware deduplication	No	Yes
Email deduplication	Attachments only	Messages and attachments
Visibility and Control Over End-User Data		
Data loss prevention (DLP)	No	Yes
Cloud applications	No	Microsoft Office 365 (Box, Google Drive coming soon)
eDiscovery enablement	No	Yes
Proactive compliance	No	Yes
Mobility and BYOD Support		
Multi-device ownership	No, licensed per device	Yes
Mobile apps	Tablets only	Smartphones and tablets
Self-deploy and self-restore	Self restore only	Yes
Data backup for smartphones and tablets	No	Yes
Global Mass Deployment		
Silent deployment	Yes	Yes
No custom scripting required	No	Yes
Installation and Management		
Installation time	Days	Minutes
1-click configuration	No	Yes
Centralized administration	Yes	Yes
End-user Experience		
Bandwidth caps	Yes	Yes
Percentage-based bandwidth throttling	No, only maximum bandwidth caps	Yes
CPU throttling	No	Yes
WAN optimization	No	Yes
Data Protection		
Manual and automatic backups	Yes	Yes
Continuous data protection	Daily	Minutes
System and application settings backup	No	Yes
Systems and application settings backup	No	Yes
Integrated enterprise file sync and share	No	Yes

About Druva

Druva is the leader in converged data protection, bringing data center class availability and governance to the mobile workforce. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.