



Protecting your endpoints and providing governance for your corporate data

Do you have a workforce that is mobile, or spread across multiple locations with multiple devices? How do you ensure that the workforce is compliant with your IT and organization security policies as well as backing-up the data that is important to them?

Druva inSync deals with these challenges by providing secure backup capabilities across multiple platforms and devices, as well as addressing your organizations need for data governance and legal compliance.

Unlimited Storage Option

Your users are busy and don't always remember to back up their critical data until it is too late! The Druva inSync client is policy driven and can be pre-configured or user managed to control which data you want protecting. Worried that you users will still exceed their storage quota? We provide unlimited storage per user*, ensuring all your data can be backed up all the time, along with simple and easy backup and restoration functionality for both users and administrators.

IT Administrators can control their estate and users, simply and effectively

Create policy-based settings for different users and groups within your organization to control how and when data is backed-up across your endpoints. You decide how much control your users have with their data and devices allowing you to enforce security, without impacting on productivity.

Lost a device? Geo-locate or remote wipe the device or just the critical corporate data, ensuring that it does not get into the wrong hands.



Ensuring the governance needs of the business are achieved

Druva inSync unifies your data into a secure central repository, ensuring that it is protected against loss and breach while giving IT full visibility for data governance. Administrators have federated search capabilities, allowing you to identify where files are stored as well geographic location of the devices. The use of pre-defined and user created compliance polices, also allow you identify and report on users and that may have sensitive or non-compliant data stored on devices or shared with other users.

React to any internal compliance breach or external legal issues by placing legal hold on data, which is collected and preserved, to be securely analyzed internally or via an external eDiscovery platform.



Enable your workforce to use their own devices without compromising on security with policy driven settings for BYOD.



Further protect and backup your Office 365 or other cloud storage to allow snapshot backup and restore capabilities to users as well as enforcing compliance and governance across cloud application data.



Enable hassle free device and OS upgrades with persona backup and restore, ensuring all your data and settings are transferred to your new device.



Enterprise grade encryption in-transit (256-bit SSL) and at-rest (AES 256) with industry first two factor encryption key management and integrated DLP functionality for device geo-locate and remote wipe capabilities.



Global data-based deduplication enables smaller faster backups by eliminating data redundancies across users, resulting in up to 80% bandwidth savings.