Frequently Asked Questions about Druva inSync

What business challenge does Druva inSync solve?

Druva inSync solves business challenges related to endpoint data protection and governance, including data backup and restore, governance (visibility, control, and eDiscovery enablement), DLP, and file sync and share.

How does Druva inSync protect corporate data against breach after device theft or loss?

Druva inSync provides complete data loss prevention including data encryption on endpoint devices, geo tracking of devices, remote wipe on laptops and mobile devices, and restore of user data, preferences, and system settings.

How does Druva inSync address eDiscovery?

Druva inSync enables eDiscovery for data stored on endpoint devices. inSync offers a complete governance solution for endpoint data including a legal hold workflow that provides identification tools with federated search and audit trails, collection and preserve-in-place capability, and eDiscovery enablement with direct access to Druva from an eDiscovery platform.

How does Druva inSync address bandwidth costs when an entire organization backs up data?

Druva inSync is architected for data storage efficiency. inSync's global, app-aware deduplication delivers up to 90% in storage and bandwidth savings, which has the added benefit of providing a better end-user experience with up to 6x faster incremental backups than any competitor. Druva accomplishes this by deduplicating blocks of data across all users in an enterprise, each subsequent user transfers and stores less data until maximum efficiency is achieved.

What if our organization needs backup in remote locations where bandwidth is a challenge?

Druva inSync offers accelerated backups and restores with CloudCache, an on-premise software appliance that delivers LAN-like speeds to local users, and helps optimize WAN usage by syncing to the inSync Cloud during off-peak hours. CloudCache provides the same global deduplication benefits as inSync Cloud, locally, by only storing deduplicated data, while storing meta-data in the Cloud. This also enables users to seamlessly move from on-premise to the WAN without disrupting backups or restores.

How does inSync manage device refreshes for all users?

Druva inSync provides a complete set of tools to accomplish large-scale device refreshes and OS migrations across endpoint devices. Features include mass deployment support for SCCM and Casper, data and persona backup for capturing and restoring of user preferences and system settings, and wizard-based workflows to enable both user- and IT-initiated device refreshes with minimal overhead and manual involvement.

What other implementation costs do I need to be aware of?

With inSync's unique Integrated Mass Deployment (IMD), delegated administration, and deep directory integration for AD save up to 75% in deployment time.

How can users be ensured of high data privacy, even from administrators?

Druva inSync offers a complete set of privacy settings required by any global enterprise. inSync enables IT to set group policies that allow users to prevent administrator access to their data, for example officers of the company. In the case of litigation, provisions can be made to enable legal department access only.

How can Druva secure against data loss?

Druva inSync Cloud has a guaranteed SLA of 99.99999% data durability, which includes up to 3-way data redundancy across data centers. Send your data only once; redundancy is automatic and transparent at no additional cost.

How secure and private is corporate data in the cloud?

Druva inSync offers a unique and highly secure 2-factor encryption scheme. By utilizing this model, no one except the customer can access their data, not even Druva. This enables companies to have complete data security and privacy: data cannot be handed over if subpoenaed or a government request is made to Druva. In addition, we feature a published vulnerability assessment, pen tests, data scrambling, and compartmentalization to ensure the greatest levels of data security and privacy for our customers.

What certifications does your cloud service comply with?

The Druva inSync cloud is up to date with the latest in infrastructure and application security and compliance, currently complying with SOC 1 (SSAE 16, ISAE 3402, formerly SAS 70), SOC 2, SOC 3, ISO 27001, PCI DSS Level 1, ITAR, HIPAA, FedRAMP, FIPS, FISMA, and others. To learn more, please contact us directly.

What is the published SLA (Service Level Agreement) for uptime?

Druva inSync is built on Amazon Web Services (AWS), which provides an SLA of 99.5% uptime across it's 10 regions and availability zones.

How about global deployment? What about regulatory implications?

Druva inSync has a global footprint across Americas, APAC, EMEA with 10 regions and 50+ edge locations across the globe and complies with EU safe harbor regulations. For regional data protection requirements, Druva inSync enables administrators to map users via profiles to regions, ensuring your data resides in the location required.

How is inSync innovating with its cloud service?

inSync was built for the cloud and delivers unique innovations with it's patented global deduplication engine, 2-factor encryption, and cloud-based storage architecture. We also provide this same approach for our on-premise customers, including support for object storage to deliver cloud-like elasticity on-premise. Furthermore in the cloud, AWS provides innovations such as Cloudfront, Glacier, redundant data center architecture, and S3 object storage, providing customers not only cost efficiencies, but more effective ways to manage data over time.

Why is global deduplication so important? Storage continues to get cheaper by the day.

Global deduplication delivers not only substantial storage savings, but also tremendous bandwidth savings: as high as 90% with significantly faster incremental backups (up to 6x faster). These bandwidth savings, coupled with resource throttling on the client lowers the impact to network bandwidth and minimizes client resource consumption, creating a better overall user experience.

How often does Druva inSync backup files?

Druva is fully configurable via administrative profiles that map to groups of users. These profiles provide advanced settings, such as backup frequency, which can be set to happen as often as every few minutes, to provide continuous data protection. If authorized by IT, end users can modify their backup schedules as needed to best fit their requirements.

How safe is my organization's encryption key?

Utilizing our 2-factor encryption scheme, Druva's approach to encryption key management ensures data cannot be lost or corrupted, as only an encrypted token is stored per user. This model prevents others outside your organization from having access to your data, a known problem when both the key and data are stored in the cloud. With AWS's 99.99999% data durability, the encrypted key data is safely stored, and as an added precaution, admin/user credentials can also be reset if required.

Learn more about Druva's security.

Will my data remain in its country of origin?

For customers requiring their data to stay in the country of origin, in order to be in compliance with regional data regulations, Druva provides full customer control over regional data storage assignments per user via profile settings. Customer data stays where it's intended and doesn't move out of that region without the customer explicitly doing so.

What type of cloud does Druva support: public, private, or hybrid?

Druva offers public, private, and hybrid cloud options.

What type of reporting features does inSync provide?

Druva provides advanced out-of-the box reporting capabilities, including a comprehensive, rich set of in-system reporting with exporting functionality.

How many concurrent backups does Druva support?

Druva has no limitations on concurrency and provides enterprise-level scale into the 100's of 1000's of users, both on-premise and in the cloud.

About Druva

Druva provides integrated data protection and governance solutions for enterprise laptops, PCs, smartphones and tablets. Its flagship product, inSync, empowers an enterprise's mobile workforce and IT teams with backup, IT-managed file sharing, data loss prevention, and rich analytics. Deployed in public or private cloud scenarios or on-premise, inSync is the only solution built with both IT needs and end-user experiences in mind. With offices in the U.S., India and United Kingdom, Druva is privately held and is backed by Nexus Venture Partners, Sequoia Capital and Tenaya Capital. For more information, visit **www.Druva.com.**

druva

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