

Druva SaaS Data Protection for Remote Office and Branch Offices (ROBO)

The challenge

Remote and branch offices are critical to the success of many organizations. These offices maintain data locally for a variety of reasons, including application design, data size, bandwidth limitation, and more. Whether expanding due to M&A or reducing size due to a divestiture, traditional on-premises data protection for remote offices is impractical. Sending people and equipment to three, five or 100 remote offices to deploy and configure data protection is time consuming and expensive. Depending on the location, getting data offsite for disaster recovery purposes and off the corporate network for ransomware protection adds even more complexity and costs.

The solution

SaaS data protection allows customers to quickly deploy, easily manage, and automatically secure backups with lower cost. By starting in the cloud, organizations gain the flexibility of on-demand storage capacity and compute that deploys in measured amounts or at scale across many offices simultaneously. Delivered as-a-service, the Druva Cloud Platform offers high-performance, scalable all-in-one backup, disaster recovery (DR), archival and analytics to simplify data protection, which dramatically reduces both complexity and costs.

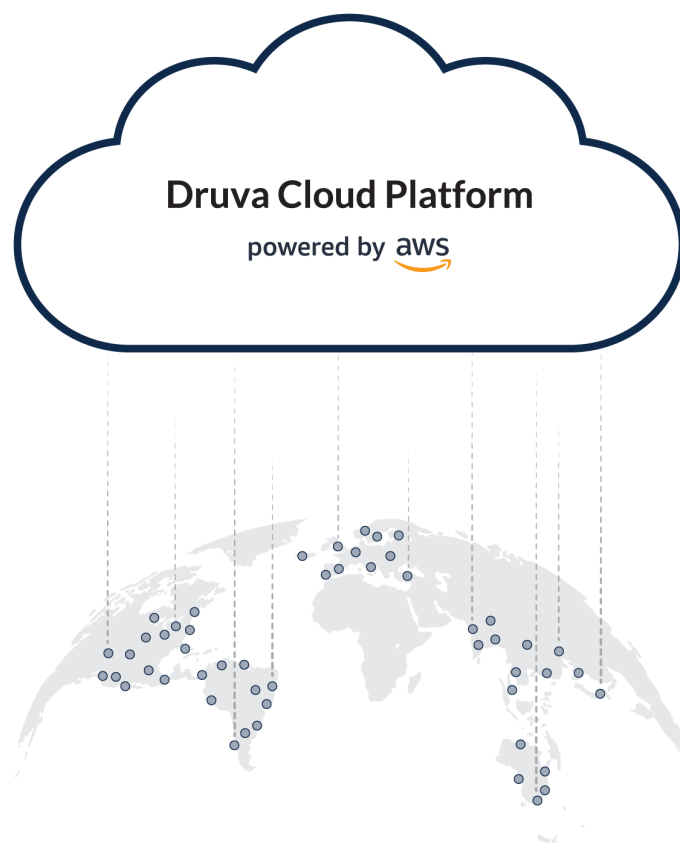
Leveraging cloud data protection does not mean sacrificing SLAs or a requirement for large amounts of bandwidth. In remote offices where bandwidth may be limited or constrained, customers can use CloudCache, a feature that stores data locally before syncing it to the cloud. CloudCache enables more frequent backups when bandwidth is limited, as well as local recovery. Customers simply deploy a software appliance based on the needs of individual offices, and because a gold copy of data lives in the cloud, customers are not dependent on local hardware for restores (or backups). Druva empowers organizations to achieve aggressive SLAs, reduce total cost of ownership (TCO) up to 50%, and secure their backup data against ransomware.

Business challenges

- High cost to deploy and manage backup, recovery, and DR across distributed sites
- Complexity and time to deploy, manage, and secure infrastructure across sites
- Reliability of backup, recovery and DR processes
- Inability to confidently protect remote office backups from ransomware

Key benefits

- Reliable ROBO data protection that deploys in minutes
- Up to 50% lower TCO for ROBO data protection
- Protects remote office backups from ransomware



How it works

Druva data protection for remote offices can be deployed quickly and easily via web browser. Role-based access control makes it easy to assign various levels of access to data and functions across teams. Support for single sign-on (SSO) and multi-factor authentication (MFA) provide the security and control needed to easily manage at scale. Efficient, direct-to-cloud backup is driven by source-side, global deduplication which reduces bandwidth requirements and storage consumption at first backup. In just a few steps, organizations create regional and global policies to establish consistent RPOs, define backup frequency and retention, and designate a data storage region. Support for 14+ AWS storage regions simplifies meeting data residency requirements.

For ROBO locations with limited bandwidth or demanding recovery-time objectives (RTOs), the Druva CloudCache feature can provide a local backup and recovery target managed within the Druva Cloud. The software appliance can be easily deployed on physical or virtual systems, and scaled up or down as needed.

Organizations can meet both daily recovery requirements and enable cloud disaster recovery capabilities using one-click, orchestrated failover (and failback) of VMware systems in minutes. With Druva, organizations get the power of a data center solution in their remote offices with the simplicity and ease of use expected from a well designed SaaS application. Druva helps organizations reduce the cost and complexity of ROBO data protection, improve business resilience, and increase IT agility.

The benefits

- **Reliable ROBO data protection that deploys in minutes** – SaaS data protection can be deployed centrally to remote offices without the need for local hardware, software, or management.
- **Up to 50% lower TCO for ROBO data protection** – Deployment, management, maintenance, and security of ROBO data protection is easier and less costly with SaaS data protection.
- **Protects remote office backups from ransomware** – Securely move and store backup data offsite, isolated from your network.

- **Single platform to protect workloads on servers, in the cloud, and on endpoints** – Centralize management and security with role-based access controls (RBAC), single-sign-on (SSO), and multi-factor authentication (MFA).
- **Predictable, utility based pricing** – Eliminate surprise costs with consumption analytics and a simple licensing model offering full system or file-level restores with no egress or “put” fees.
- **Fast, efficient backup and recovery** – Source-side, global deduplication (petabyte scale) and incremental forever backups drive significant network and storage efficiencies.
- **Cloud disaster recovery** – Customers automatically have an offsite data copy, eliminating the need for replication or tape. Druva DRaaS enables automated and orchestrated failover of VMs into a customer VPC in minutes, allowing a higher level of resilience at a much lower price (vs. typical replication).
- **Data archiving and long-term retention** – Integrated long-term retention capabilities allow both automated storage tiering (warm to cold) as well as direct- to-cold storage backups, making it easier and less expensive to meet compliance requirements.
- **API-based integrations** – Automate and extend enterprise applications with API-based integrations. RESTful APIs enable integration with third party applications. ServiceNow integration automates service help desk ticket creation to resolve IT requests and issues faster.
- **Data security and privacy certifications** – Druva utilizes 256-bit AES encryption for data at rest and TLS 1.2 for data in transit, and meets a number of certifications including SOC-2 Type II, HIPAA, Privacy Shield compliance, and ITAR (U.S. GovCloud only).

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300

Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva is the industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a \$10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).