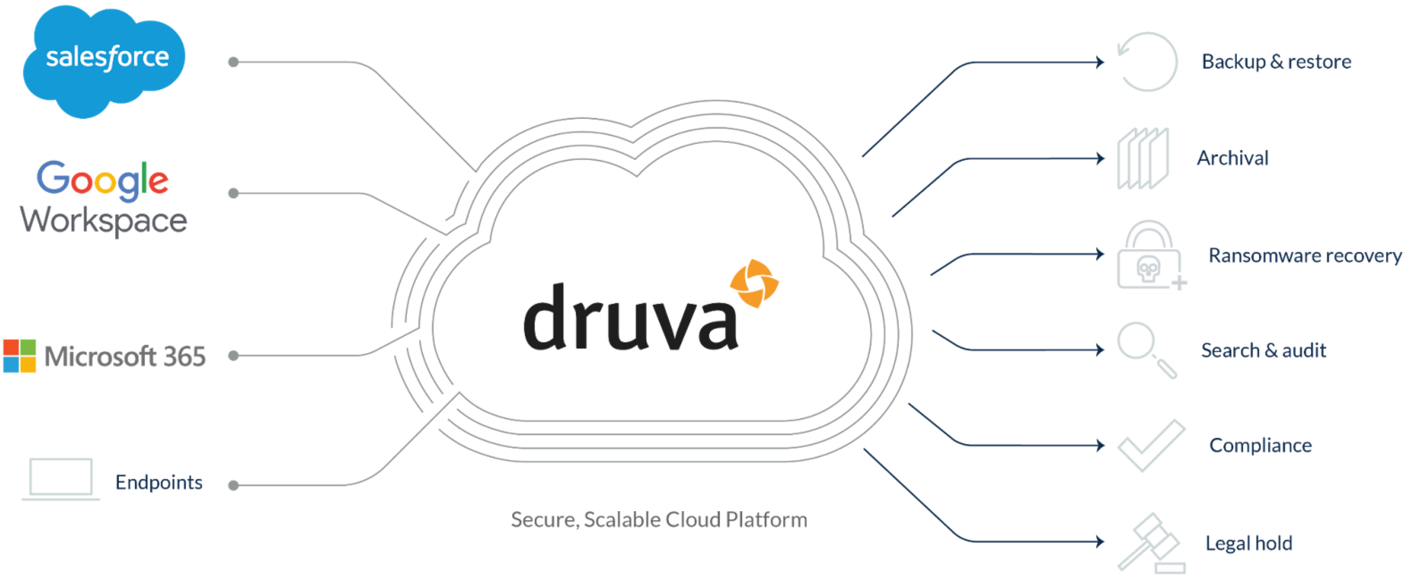
Druva Data Security for SaaS Applications & End-User Devices

Workforce mobility and the rise of cloud services are an essential part of modern business, but create a number of challenges for IT. User data spread across devices and SaaS services, unpredictable schedules, and varied network connections all complicate efforts to protect and govern enterprise information.

Druva is a 100% SaaS platform that delivers unified data security, management, and information governance at scale across endpoints and cloud applications in a secure and compliant manner. Delivered as-a-service, Druva simplifies backup, archival, recovery, and device management to reduce the cost and complexity of protecting end-user data, support regulatory compliance, and improve data visibility.



Why Druva?

SaaS application data protection

Druva's SaaS platform provides comprehensive data security to mitigate data loss risks such as accidental and malicious deletion and ransomware attacks across multiple SaaS workloads, including Microsoft 365, Google Workspace, and Salesforce with automated and centrally-managed backup and flexible recovery options. Our SaaS data security provides the same cloud benefits that led you to choose a SaaS application, such as cloud scale, cost efficiency, and agility. A SaaS solution like Druva, with regular over-the-air feature updates, is best positioned to support the innovation rate and velocity of SaaS applications.

Endpoint data protection

Druva is a performant and versatile service that facilitates backup, security, and recovery of data located on end-user devices, to mitigate data loss and intellectual property theft. Backups run in the background with no disruption to the end user. Druva provides bulk and granular recovery options that can be centrally managed by IT or delegated to end-users through an easy-to-use self-service experience. This ensures business continuity in the face of accidental or malicious data loss and ransomware attacks. Data on stolen devices can be remotely wiped even without an internet connection, proactively preventing theft of proprietary and confidential information.

Data compliance monitoring

Druva is the only integrated solution that brings visibility to end-user data and provides an automated system to proactively track, monitor, and notify of potential data compliance risks. With process automation for identifying files that may contain sensitive information, IT can quickly assess and take corrective action for non-compliance of end-user data across the industry's highest standards, including SOC2 type II, HIPAA, FIPS 140-2, and FedRAMP ATO.

Threat hunting

Druva's threat hunting solution enhances incident response by searching for threats across an extended timeline of backups and all end-user data, including endpoint devices and apps like Microsoft 365 and Google Workspace. Via the Druva console, locate and quarantine threats to prevent the restore of compromised data and eliminate reinfection risks, while also destroying threats from backups and primary environments through defensible deletion.

Legal hold and eDiscovery enablement

Druva facilitates completeness of data discovery for legal purposes by allowing admins to centrally collect and preserve dispersed enterprise data across endpoints and SaaS applications, cutting time required for eDiscovery in half. Tight integration with third-party tools and speedy downloads accelerate the data collection and delivery process. Through automated legal hold workflows, chain of custody reporting, extended metadata, and file fingerprinting, Druva ensures authenticity and alignment with EDRM and Department of Justice requirements.

OS migration and device refresh

With an accessible dashboard, Druva allows IT to manage the entire OS migration process at scale through a single interface, providing automated backups of both data and system settings. It protects against data loss and integrates mass deployment tools. Self-restore options reduce time and IT resources required — and anytime/anywhere access to data minimizes productivity loss during the migration process.

Integration with SIEM and identity management tools

Built-in integrations for Security Information Event Management (SIEM) automate the collection of event data from Druva and alert IT teams to important changes in their data. These include data anomalies like bulk deletions and authentication failures. It also alerts IT to issues related to security-focused use cases, such as understanding which geography restores are occurring.

Accelerated data recovery

Effective data restoration is crucial to minimize disruptions and ensure business continuity during data loss or system failure. Druva enables rapid recovery with granular restore and Curated Snapshot, capturing point-in-time backups of critical data free of infections. This ensures reliable data availability and allows for mass restores across an organization, whether it impacts a few hundred or thousands of users.

Enhanced security posture and incident response

The Druva Data Security Cloud provides comprehensive protection for end users globally, addressing both reactive and proactive security needs. It ensures high levels of security, immutability, and integrity with features including air-gapped storage, encryption, and anomaly detection. Druva offers simplified data migration, centralized visibility, and monitoring to manage and alert you to security risks, and with sandbox recovery, users can test data to prevent reinfection. Druva empowers organizations to tackle modern data risks confidently, ensuring data safety and reducing costs.

Key features

SaaS data protection

- Multiple workloads — Microsoft 365, Google Workspace, Salesforce, and endpoints
- Scale on-demand
- Up to 40% reduction in TCO vs. competing legacy, on-prem solutions
- Invisible backup windows
- End-user access with self-service restore
- Global source-side deduplication and incremental forever model enable faster backups

Compliance and data governance

- Federated search across all backup data
- User-centric legal hold
- Automated and proactive compliance monitoring for HIPAA, GDPR

Security

- Customer-only access to customer data
- AES-256 encryption for data at rest
- TLS 1.2 encryption for data in transit
- No key management required
- Certs: SOC-2 Type-II, HIPAA, Privacy Shield
- FedRAMP Authorized

Administration

- Zero administration overhead — no software install, upgrades, patches, or cluster management
- Cloud-based centralized management from a single pane of glass across workloads
- Role-based access control (RBAC)

Endpoint features

- Fast and simple OS migration/device refresh
- Integrated mass deployment for endpoints
- Single sign-on support (SAML, ADFS)
- Optional CloudCache support
- Data loss prevention (DLP) with device remote-wipe backup

Empower your business with Druva — check out the SaaS apps and endpoints product page for more insights.

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 leading provider of data security solutions, empowering customers to secure and recover their data from all threats. The Druva Data Security Cloud is a fully managed SaaS solution offering air-gapped and immutable data protection across cloud, on-premises, and edge environments. By centralizing data protection, Druva enhances traditional security measures and enables faster incident response, effective cyber remediation, and robust data governance. Trusted by over 6,000 customers, including 65 of the Fortune 500, Druva safeguards business data in an increasingly interconnected world.