Protecting Your Modern Enterprise End User

Enterprises today are tasked with protecting their data regardless of where that data resides. As users keep data locally on their device(s), in email, cloud storage, and shared drives, backups of any single repository are not comprehensive enough and leave your organization exposed.

Druva has been at the forefront of data protection, and trends in customer adoption have shown us that extending our endpoint data protection to include cloud workloads is key. With Druva, your admins access and manage backups of all endpoints and cloud workloads via one centralized and secure platform — the Druva Data Security Cloud.

Business Challenges	Key Benefits
• **Data loss:** Endpoint failure, failure to backup, accidental deletion, and data corruption • **Compliance and governance:** Missing data, PCI, and PII • **Security**: Ransomware, malware, insider threats, and undetected anomalous activity • **Restore and recovery:** Scope of data loss unknown, manual restore processes, inefficient mass restore, and insufficient backup	• **Centralized view:** Complete coverage of all end-user data across endpoints and SaaS apps • **Secure backups:** Encrypted data during transit and rest, RBAC, zero trust, data lock, air-gapped, and immutable • **Compliance:** FedRAMP-compliant, Legal hold, eDiscovery, federated search, and sensitive data governance • **Cyber resiliency:** Rollback actions, DLP, ransomware protection, curated recovery, quarantine • **Recovery:** Point-in-time, granular, secure, and mass restores

The Challenge

Hybrid work environments have necessitated significant changes in the way organizations store, secure, and restore data. For example, platforms like Microsoft 365 and Google Workspace have become key repositories for enterprises, enabling seamless collaboration and remote work. This shift brings forth challenges in data security. To protect data consistent with governance and legal requirements, organizations must implement robust data protection frameworks encompassing encryption, access controls, and user education. Simultaneously, effective planning for data restoration at scale is essential to ensure business continuity.

The Shared Responsibility Model

As an organization using collaboration tools, you are responsible for securely backing up the data stored on these platforms, as well as managing encryption, recovery, retention, identity and access policies, compliance, and security. Cloud providers like Microsoft and Google outline customer responsibilities and often recommend third-party solutions for backup. These platforms are vulnerable to human error and malicious activity, with no automation for mass or curated recovery, making them susceptible to widespread deletions or malware through synchronization. Many SaaS applications lack comprehensive recovery options, focusing only on service availability and performance, not data recovery.

The Solution

Druva delivers a centralized, fully managed 100% SaaS platform to protect your data wherever it lives — on any device, application, or cloud. Enterprises gain valuable insight into their security posture and ensure valuable data stored across devices and cloud workloads is secure, compliant, and always accessible for effortless mass restore. Customers benefit from automated secure backups, centralized management, and speedy data recovery for a seamless and reliable backup solution.

Offering	Details
Endpoints	• **Data Protection for Endpoints** – Fully automated, air-gapped backup for end-user devices (laptops/desktops), protecting endpoint data securely. • **Offline PSTs & Inactive User Retention** – Meet data security, compliance, access control, and retention requirements. • **Managed Data Detection & Response** — 24×7 managed monitoring of backup data to detect anomalies/malware early, with expert incident response. • **AI Copilots (Dru Assist & Investigate)** – AI-driven assistance for support and cyber threat investigation, providing intelligent insights and automation for endpoint data security.
Microsoft 365	• **Data Protection for Microsoft 365** – Fully managed, immutable backup for Microsoft 365 data (covering Exchange Online, SharePoint, OneDrive, Teams, Planner, etc.), ensuring business-critical M365 content is automatically protected. • **Public Folders, PSTs & Inactive User Retention** – Protection for Exchange Public Folders and PST archives, with retention of departed users' M365 data to meet compliance and legal hold requirements. • **Microsoft Entra ID Protection** – Safeguards and allows recovery of Azure AD (Entra ID) directory objects (users, groups, etc.), preventing permanent loss of identity data. • **Managed Data Detection & Response** • **AI Copilots for Data Security**
Google Workspace	• **Data Protection for Google Workspace** – Fully managed, air-gapped backup for Google Workspace apps (Gmail, Drive, Calendar, Contacts, etc.), ensuring all SaaS data (including Google Drive files like Docs, Sheets, Slides) is securely backed up. • **Shared Drive & Inactive User Retention** – Backup of Google Shared Drives and long-term retention of data from former employees, helping meet archiving and compliance mandates. • **Managed Data Detection & Response** • **AI Copilots for Data Security**
Advanced Features	• **Federated Search & Legal Hold** – Enterprise-wide eDiscovery across M365, Google, and endpoint backups, with the ability to search files/metadata and place legal holds or perform defensible deletion (available in higher-tier plans). • **Security Center** – A centralized security dashboard to monitor backup security posture, detect risks and anomalies, and guide proactive defenses (included in Elite Plus; optional add-on for lower tiers). • **Data Anomaly Detection & Integrations** – Automated detection of unusual data change patterns and suspicious access events, with alerts and integration to third-party SIEM/analytics tools via APIs. • **Quarantine Bay** – Isolated quarantine storage to hold infected or suspect backup snapshots, preventing malware reinfection during restore and allowing safe investigation of incidents. • **Curated & Orchestrated Cyber Recovery** – Automated workflow to identify clean, malware-free versions of files across backups and orchestrate streamlined recovery after a cyber attack (with support for malware scanning and scripted recovery steps).
Add-ons [each line item is sold separately]	• **Microsoft 365 Backup Express** – High-speed backup and restore capability enabling bulk recovery at 1–3 TB per hour; offered as a separate add-on for environments with large datasets. • **Sensitive Data Governance** – Advanced data governance module with pre-built templates to identify and manage sensitive or regulated data in backups, and implement policies like automated sensitive data discovery and defensible deletion (not included in standard tiers). • **U.S. GovCloud (FedRAMP)** – Deployment in Druva's FedRAMP-authorized GovCloud environment for U.S. government data compliance. This add-on provides a dedicated, FedRAMP Moderate-compliant cloud instance with full encryption for agencies or contractors requiring U.S. government cloud security standards.

Key Benefits

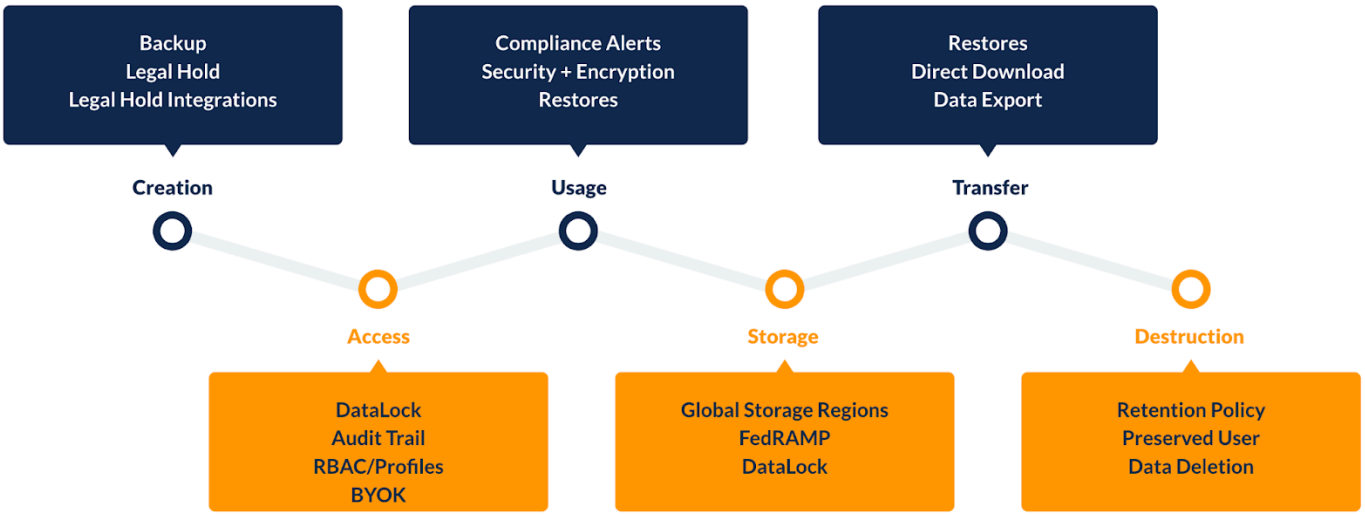
Mobility: Dispersed Data and Workforce

Druva empowers organizations to embrace mobile workforces and provides seamless access to their data, while maintaining visibility and control. This enhances user productivity by enabling quick and easy data recovery in the event of device issues or data loss and allows users to get back to work without significant disruptions.

- **Accessibility:** Druva enables end users to access their data from anywhere, at any time, on any device
- **Device Migration:** Druva simplifies data migration by quickly and easily restoring endpoint data onto a new device
- **Data Loss Prevention:** Druva prevents data loss by automatically backing up data across endpoints and SaaS apps to the cloud to the cloud

Governance and Compliance

As data is dispersed across platforms, it becomes increasingly critical to have a robust data protection framework to safeguard data and adhere to governance and compliance requirements. This should encompass policies for backup, access controls, security, compliance (i.e. PCI, PII, HIPAA), retention (i.e., industry-specific data retention regulations), legal hold, and eDiscovery. Aligned to the data lifecycle, Druva's data protection platform has built-in workflows and capabilities to help organizations navigate the complex landscape of regulatory compliance and governance. For example, with process automation for identifying files that may contain sensitive information, Druva empowers IT teams to quickly assess and take action for the non-compliance of user data. Additional governance capabilities include federated search with integrated full-text search indexing, extensive auditing, and intuitive data visibility, providing greater insight into potential data risks.



Optimized Recovery — Accelerated Data Restoration at Scale

In the event of data loss or system failure, effective data restoration is crucial to minimize disruptions and ensure business continuity. Enterprises should establish comprehensive backup and recovery strategies that encompass both endpoints and SaaS applications. Regular backups, redundant storage systems, and automated backup processes are essential components of a reliable data restoration plan. Additionally, testing the restoration process periodically helps identify and address any potential gaps.

Doing so ensures basic data availability hygiene and the ability to restore with confidence when you are impacted by a data security incident. Druva provides rapid recovery with granular restore and Curated Snapshot, a feature that allows organizations to capture and store point-in-time backups of critical data, providing a pristine snapshot that is free of infected files while providing the end user with workable copies of the latest versions. Saving time and data, Druva enables mass restore of data across your end users, whether it impacts a few hundred or thousands across your organization.

Improved Security Posture and Recovery Readiness

As the threat surface for data security expands, enterprises must be cognizant of potential vulnerabilities, including unauthorized access, data breaches, and insider threats. The distributed nature of data storage necessitates a comprehensive security strategy that encompasses encryption, access controls, multi-factor authentication, and regular security audits. Failure to address these concerns may expose sensitive client data to potential risks.

The Druva Data Security Cloud addresses the security of data for your end user — at scale and globally — be it reactively from an attack or isolated incident, or proactively as part of a device refresh cycle.

- **Foundational:** High level of security, immutability, and integrity in backup services, ensuring protection from malware and ransomware with features including air-gapped storage, encryption, and anomaly detection.
- **Security Posture and Observability:** Simplified data migration for quick and easy restore of endpoint data to new devices, ensuring a seamless and secure transition. Druva provides centralized visibility, control, and monitoring of data across endpoints, cloud environments, and SaaS applications to effectively manage and alert you of security risks.
- **Accelerated Ransomware Recovery:** Rapid recovery from ransomware with point-in-time restores, automated detection, and response to minimize data loss, reduce downtime, and simplify the recovery process with centralized management and intelligent analytics.

Druva empowers organizations to protect their end user regardless of where the data resides — on your users' devices or in SaaS applications — so you can confidently tackle modern data risks such as security threats, data loss, compliance requirements, and management complexity, all while reducing costs. With Druva, your data is always safe and always ready.

druva Sales: +1-800-375-0160 | sales@druva.com

Americas: +1-800-375-0160
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. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.