

# Protecting Your Modern Enterprise End User

Enterprises today manage data that is distributed across various devices and collaboration platforms. These organizations 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
<ul style="list-style-type: none"> <li>• <b>Data loss:</b> Endpoint failure, failure to backup, accidental deletion, and data corruption</li> <li>• <b>Compliance and governance:</b> Missing data, PCI, and PII</li> <li>• <b>Security:</b> Ransomware, malware, insider threats, and undetected anomalous activity</li> <li>• <b>Restore and recovery:</b> Scope of data loss unknown, manual restore processes, inefficient mass restore, and insufficient backup</li> </ul>	<ul style="list-style-type: none"> <li>• <b>Centralized view:</b> Complete coverage of all end-user data</li> <li>• <b>Secure backups:</b> Encrypted data during transit and rest, RBAC, zero trust, data lock, air-gapped and immutable</li> <li>• <b>Compliance:</b> FedRAMP-compliant, Legal hold, eDiscovery, federated search, and sensitive data governance</li> <li>• <b>Cyber resiliency:</b> Rollback actions, DLP, ransomware protection, curated recovery, quarantine</li> <li>• <b>Recovery:</b> Point-in-time, granular, secure, and mass restores</li> </ul>

## 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 with end users of these collaboration tools, you are responsible for ensuring the data stored in these platforms is securely backed up. Additionally, the customer is responsible for encryption, recovery, retention, identity and access management policies, compliance, and security. Cloud platforms like Microsoft and Google clearly identify the responsibilities of their customers as well as recommend using a third-party solution for this purpose.

These collaboration platforms are not immune to human error or malicious activity, and there is no automation for mass or curated recovery — this leaves them susceptible to a wildfire-like spread of deletions or malware through synchronization. Many SaaS applications do not include easy-to-use or comprehensive recovery options and only guarantee the availability and performance of the service — not 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
Endpoint + Microsoft 365	<ul style="list-style-type: none"><li>• One license for Endpoints and one license for Microsoft 365</li><li>• Shared mailbox: 50% of Microsoft 365 licenses</li><li>• Storage: 50GB for Endpoint licenses and 50GB for Microsoft 365</li><li>• Preserved users: 10% of Endpoint licenses and 10% of Microsoft 365 licenses</li></ul>
Endpoint + Google Workspace	<ul style="list-style-type: none"><li>• One license for Endpoints and one license for Google Workspace</li><li>• Storage: 50GB for Endpoint licenses and 50GB for Google Workspace licenses</li><li>• Preserved users: 10% of Endpoint licenses and 10% of Google Workspace licenses</li></ul>
Advanced Security End-User Bundle	<ul style="list-style-type: none"><li>• Endpoint + Microsoft 365 or Endpoint + Google Workspace</li><li>• <a href="#">Accelerated Ransomware Recovery</a></li></ul>
Add-ons <small>[each line item is sold separately]</small>	<ul style="list-style-type: none"><li>• One license for Endpoints and one license of Microsoft365 / Google Workspace for the following add-ons:<ul style="list-style-type: none"><li>◦ Preserved User</li><li>◦ Sensitive Data Governance</li><li>◦ GovCloud</li><li>◦ Core <a href="#">SP&amp;O</a> — visibility, monitoring, and incident response</li><li>◦ <a href="#">Advanced Ransomware Recovery</a> for accelerated cyber recovery</li></ul></li><li>• Unlimited Storage: One unit provides 250GB of additional storage as part of storage pool</li></ul>

Key Benefits

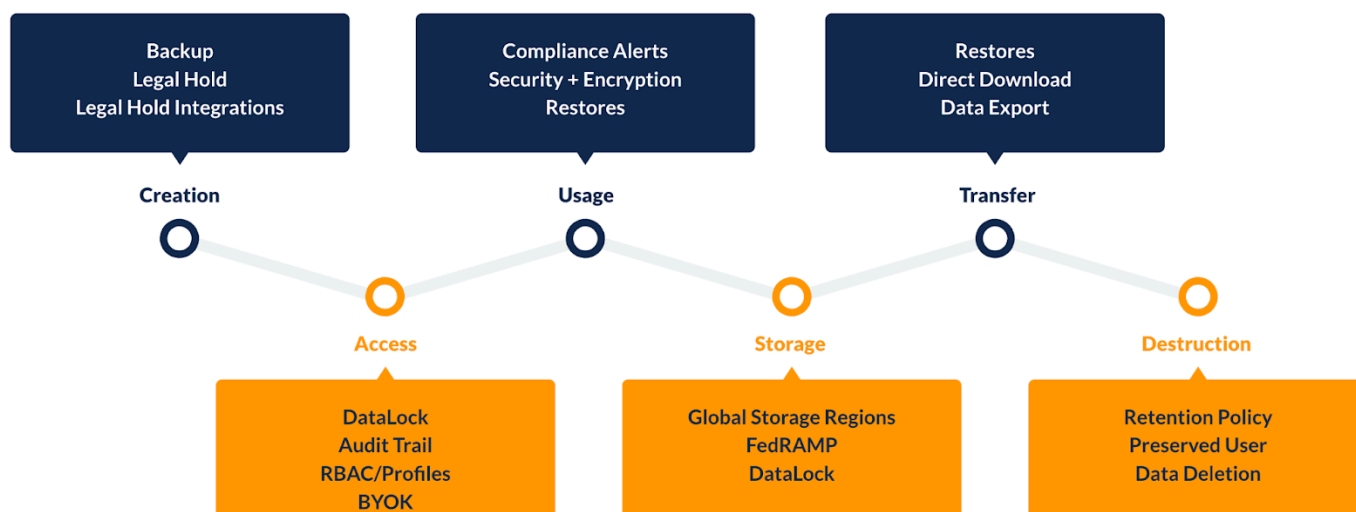
Mobility: Dispersed Data and Workforce

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 end-user data onto a new device
- **Data Loss Prevention:** Druva prevents data loss by automatically backing up end-user data 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

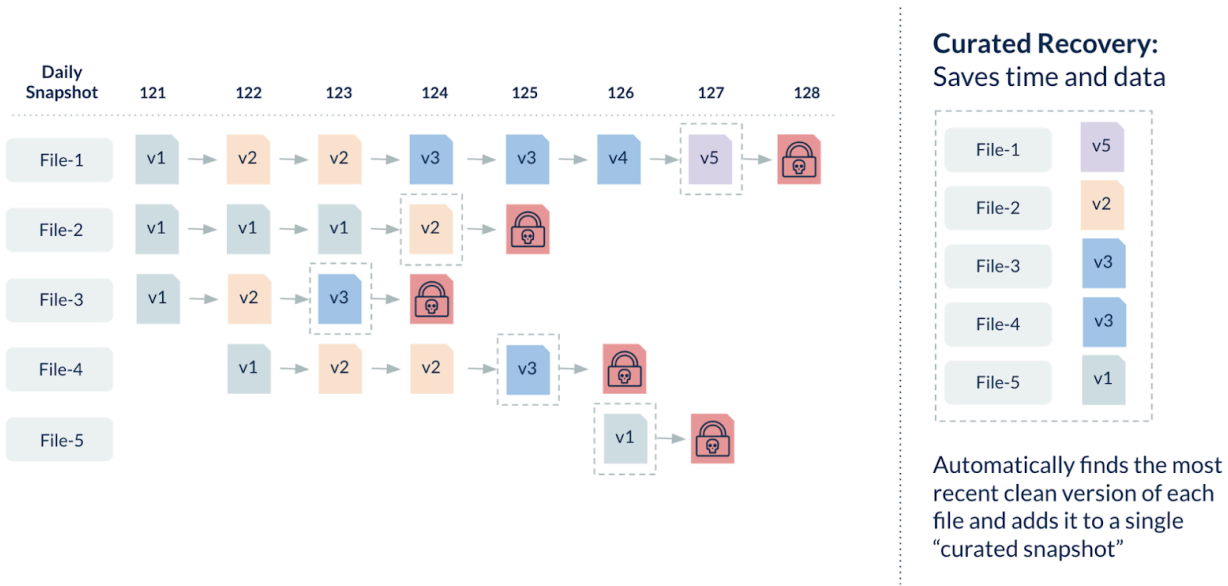
In the event of data loss or system failure, effective data restoration is crucial to minimize disruptions and ensure business continuity. Enterprises should establish comprehensive backup and recovery strategies that encompass both endpoints and SaaS applications. Regular backups, redundant storage 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 end-user 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 user’s device or in M365 — 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.


Spotlight on Customer Success



Managing and building homes

**Thirteen** — Thirteen successfully protects all endpoint and Microsoft 365 data from accidental deletion and ransomware using Druva, finding it’s now 100% secure and recoverable with a 95% faster recovery process.

[Learn more in the case study.](#)



**Sembcorp** — Sembcorp effectively secured over 3,000 endpoints and addressed Microsoft 365 gaps with Druva, resulting in improved endpoint security and

accessibility with 12x faster data restores vs. its previous Microsoft-only solution. [Learn more in the case study.](#)



Sales: +1-800-375-0160 | [sales@druva.com](mailto: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](mailto:japan-sales@druva.com)  
Singapore: [asean-sales@druva.com](mailto:asean-sales@druva.com)  
Australia: [anz-sales@druva.com](mailto: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](https://druva.com) and follow us on [LinkedIn](#), [Twitter](#), and [Facebook](#).