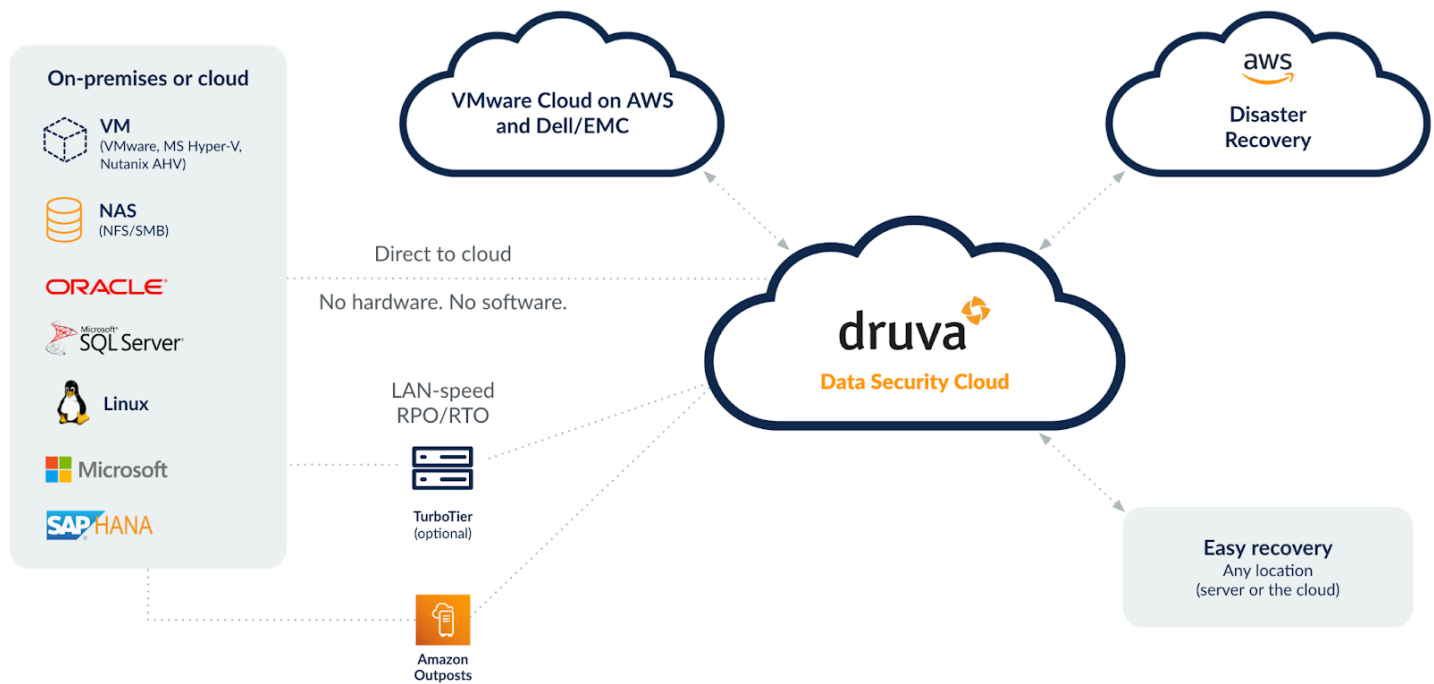


Cyber Resilience for Hybrid Workloads

Organizations adopting a cloud-first approach face limitations with traditional data protection, including high costs, complex management, and weak defense against advanced threats like ransomware. Additionally, these legacy systems often fail to provide visibility, integrated security, and the agility required in today's hybrid environments. The data center remains foundational, requiring standardized cyber resilience to meet compliance at scale. Druva offers a radically simplified approach to protecting and managing data across diverse hybrid workloads. With automated ransomware detection, curated clean recovery, and always-immutable backups, Druva ensures organizations can restore with speed and confidence.



Why Druva for Hybrid Workloads?

Unified Protection Across Diverse Workloads

Leverage Druva's unified platform to seamlessly protect data across physical servers, virtual servers (VMware, Hyper-V, Nutanix AHV), hybrid cloud infrastructure (VMware Cloud), NAS or cloud file storage, and databases (MS-SQL, Oracle, SAP HANA). Streamline data protection management from a single console.

DruAI for VMware

Harness the full potential of AI with DruAI-powered agents to intelligently guide and automate the VMware restore process — including investigation, policy validation, and execution.

Advanced Cyber Resilience

Druva's solution goes beyond traditional backup, delivering comprehensive ransomware protection and recovery capabilities, including:

Air-Gapped and Immutable Backups: Isolate backup data from primary environments to protect against ransomware, accidental deletion, and insider threats. Ensure data immutability with secure encryption and strict access controls.

Threat Insights: Druva Threat Watch automates scanning and quarantine of backup snapshots for early threat detection and recovery readiness. Threat Hunting provides on-demand metadata searches to identify, isolate, and remove infected backup points for clean recovery.

Accelerated Ransomware Recovery: Rapidly recover clean, unaffected data, minimizing downtime through curated snapshots and automated anomaly detection. Quickly restore operations from trusted, verified recovery points.

Security Posture and Observability: Gain real-time insights into backup security, detect unusual data activities, and respond faster with integrated observability dashboards. Enhance security posture with continuous monitoring and actionable alerts.

Managed Data Detection & Response (MDDR) with Safe Mode: A fully managed service offering 24/7 security monitoring and threat detection for your backup environment. If a breach is suspected, Safe Mode locks down your environment to contain threats. The Druva Incident Response team quickly verifies threats, restricts access, and assists customers with response and recovery to minimize impact and speed resolution.

Key Features

Data Backup and Recovery

- Incremental-forever backups with unlimited restore points
- Global, source-side deduplication (reducing bandwidth usage by up to 80%)
- High-speed LAN-based backup and restore via TurboTier
- Granular file-level search and recovery across snapshots

Administration and Compliance

- Centralized, cloud-based management
- Unified interface for hot, warm, and cold storage management
- Automated long-term retention with auto-tiering for regulatory compliance
- Actionable, predictive analytics for storage optimization

Multi-Cloud and Hybrid Cloud Support

- Seamless integration with AWS and Microsoft Azure environments
- Cross-region and cross-cloud data protection capabilities
- Support for diverse deployments: cloud-native, hybrid, and multi-cloud

Enhanced Data Security

- Immutable, air-gapped backups with advanced encryption (AES-256, TLS 1.2)
- Zero-trust architecture with role-based access control (RBAC)
- SOC-2 Type II, HIPAA, Privacy Shield, and FedRAMP-moderate certifications

Disaster Recovery (DR)

- One-click failover and failback with automated runbook orchestration
- Rapid failover with minimal RTO and RPO
- DR into customer-owned VPCs or cloned VPCs across regions/accounts
- Curated recovery to non-disruptively scan backups for malware before restoration, slashing recovery times from days to hours.

Data Archiving

- Lower costs for compliance with both auto-tiering to cold storage and direct backups to archive storage
- No limitation to the number of aged snapshots
- Shared global dedupe index for lower-cost, long-term storage

Customer Benefits

Simplified Deployment

- Fully SaaS-based, Druva eliminates complex setups and deploys in minutes, safeguarding data quickly with no infrastructure or upfront costs.

Improved Visibility and Control

- Get complete oversight with a unified interface. Simplify monitoring, boost control, and make smarter decisions with detailed workload visibility.

Reduced Complexity and Cost

- Reduce total cost of ownership by up to 40% by eliminating hardware, employing global deduplication, auto-tiering to cost-effective storage, and leveraging a consumption-based model with no egress charges.

Rapid, Reliable Recovery

- Minimize downtime and protect critical data with Druva's advanced recovery, ensuring fast restoration and business continuity.

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 industry's leading SaaS platform for data security, 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 Security 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](#).