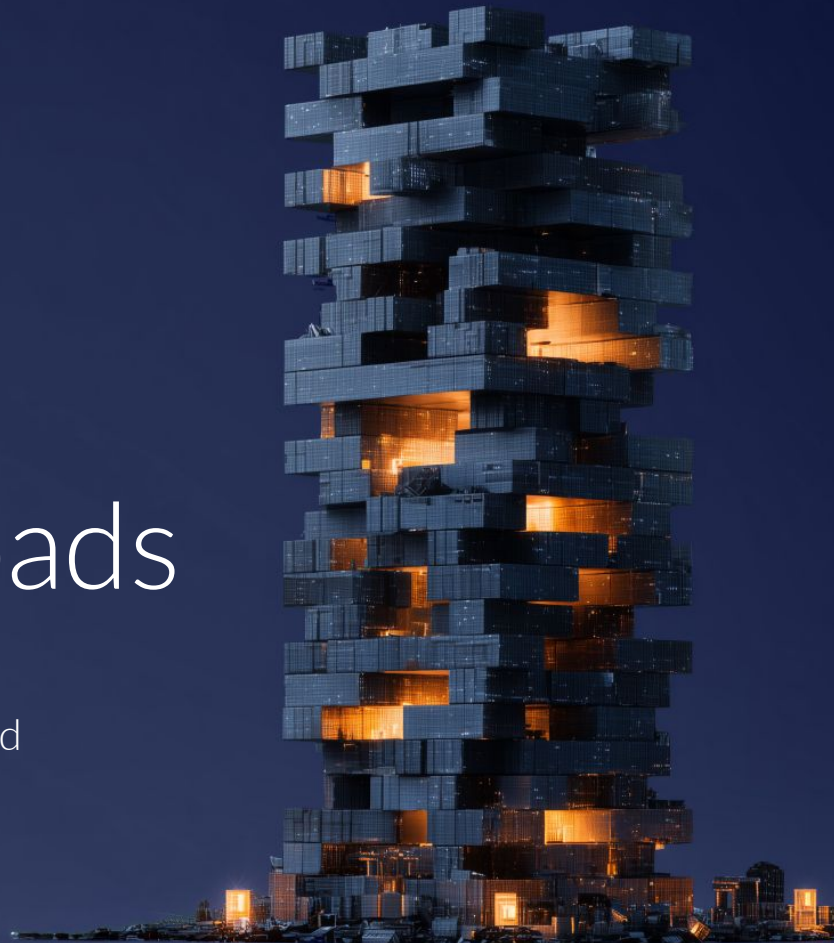




Securing Modern Data Centers & Distributed Workloads

Real customers. Real results.

Simplify Data Protection, Enhance Cyber Resilience, and
Achieve Local Performance for Distributed Workloads.



A tall, dark, modular tower structure composed of many stacked, rectangular blocks. The tower is illuminated from within, with a warm orange glow emanating from several levels, creating a stark contrast with the dark exterior and the deep blue night sky. The base of the tower is more complex, with various smaller structures and lights visible.

Table of Contents

[Modern Environments Are Distributed by Design](#)

[The Failure of Traditional Data Protection](#)

[The Urgent Need for Cyber Resilience](#)

[Case Study 1: BW Offshore](#)

[Case Study 2: NSI](#)

[Case Study 3: Paradise Group](#)

[Case Study 4: Elmet Technologies](#)

[Case Study 5: Betenbough](#)

[How Druva Delivers Radical Simplicity](#)

[Advanced Security & Recovery Capabilities](#)

[Next Steps](#)

Modern Environments Are Distributed by Design

Modern organizations are adopting a cloud-first approach, but their data remains diverse. From physical servers and VMware clusters to cloud workloads and remote sites, IT teams must protect data across environments that weren't designed to work as one.

- **The Foundational Data Center:** The data center remains the bedrock of modern infrastructure, requiring standardized resilience to meet compliance at scale.
- **A Cloud-First Approach:** Organizations are increasingly adopting cloud-first strategies to improve agility and scale.
- **Diverse Workload Demands:** Modern environments must support a mix of physical servers, virtual machines (VMware, Hyper-V, Nutanix), and cloud-native databases.
- **Distributed Complexity:** Data now lives across on-premises hardware, edge locations like Amazon Outposts, and multi-cloud platforms like AWS and Azure.

The challenge isn't whether to use SaaS —it's how to simplify protection and recovery without deploying and managing complex backup infrastructure



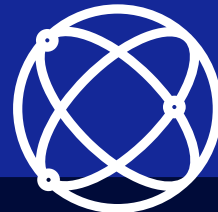
The Failure of Traditional Data Protection

- **Prohibitive Costs:** Traditional backup still requires backup servers, storage targets, and replication infrastructure. Capacity planning, hardware refresh cycles, and maintenance contracts drive TCO higher over time.
- **Management Complexity:** Even when storage moves to the cloud, IT teams still patch backup servers, scale storage, and troubleshoot performance across data center and remote environments.
- **Expanded Attack Surface:** Backup servers and storage deployed on-premises can become accessible during ransomware attacks putting recovery points at risk.
- **Operational Silos:** Separate tools across data center, cloud, and remote sites create inconsistent policies, fragmented visibility, and slower recovery.



The Urgent Need for Cyber Resilience

- **Beyond Simple Backup:** In a world of sophisticated attacks, simply having a copy of data is no longer enough; organizations need simplified management and trusted recovery.
- **Ransomware Readiness:** Automated detection and verified clean recovery are essential to restoring operations with speed and confidence.
- **Regulatory Pressure:** Meeting compliance requires automated long-term retention and air-gapped security to prevent accidental or malicious data loss.
- **Business Continuity:** Minimizing downtime through rapid failover and failback is critical for maintaining 24/7 operations.



BW Offshore Achieves 80% Time Savings for Nutanix & Hyper-V Backups with Druva

BW Offshore Limited is a global owner and operator of floating production, storage, and offloading (FPSO) vessels. The company is listed on the Oslo Stock Exchange. The company has its headquarters in Singapore and Oslo, Norway, but operates internationally. The largest shareholder is BW Group Limited, holding 49.3% of the shares.

The Challenge

- BW Offshore's legacy backup system was resource intensive, required manual intervention, and failed to meet recovery SLAs.
- Managing local hardware on vessels was difficult due to limited access and caused ongoing maintenance issues.
- Satellite connectivity limitations (low bandwidth, high latency) disrupted off-site data replication and production systems.
- The IT team lacked complete data protection, needing a scalable, reliable, and simpler solution.

The Solution

- BW Offshore chose Druva becoming their first AWS-based solution in an Azure-focused environment.
- Transitioned fully to SaaS, eliminating physical backup appliances; first workload deployed within an hour.
- Druva's deduplication and optimization enabled efficient backups for diverse environments including Nutanix AHV and Hyper-V.
- Centralized dashboard allowed easy, low-overhead monitoring across locations; the solution proved secure, reliable, and easy to manage.

Highlights

- 80% reduction in time to manage backups since bringing in Druva – one day per week is reclaimed
- The platform successfully addressed its challenge of backing up data over satellite connections from its FPSO vessels.
- Deployment took just one hour, even with satellite-based bandwidth.
- Leverage Druva TurboTier for local recovery of select workloads

[Read the full customer story ↗](#)

NSi Industries Ensures Data Integrity & Reduces Insurance Costs with Druva Following Security Incidents

For over 45 years, NSi has been a trusted partner powering market-leading brands and products, dedicated to meeting the needs of distributors across the country. Guided by a commitment to service and value, NSi consistently delivers innovative, high-quality electrical and HVAC solutions that drive industry progress. As the go-to partner for distributors, NSi makes business effortless.

The Challenge

- NSi Industries struggled with legacy, on-premises backup systems including a mix of Veeam and Dell Avamar.
- Backup processes were unreliable and required manual intervention, such as an administrator taking physical tapes off-site.
- The legacy setup lacked proper air-gapping and secure protection, leaving data vulnerable.
- The team could not validate if backups were 100% complete or secure, leading to failed full-image restores for SQL servers.

The Solution

- Implemented Druva's 100% cloud-native platform to provide air-gapped backups and built-in ransomware protection.
- Deployed Druva's Accelerated Ransomware Recovery feature to ensure data integrity and rapid restoration during critical events.
- Consistently managed a diverse environment including server backups, Microsoft 365 and Azure VMs.
- Leveraged an intuitive, user-friendly admin console that simplified file restorations.

Highlights

- Successfully restored 100% of data using the Druva Data Security Cloud following security incidents in 2023.
- Secured a 25% discount on cybersecurity insurance premiums by implementing Druva's advanced security features.
- Streamlined backup and restoration processes, achieving faster restore speeds for both AWS and hybrid environments.

[Read the full customer story ↗](#)

30% Reduced TCO & Cloud-Based Cybersecurity: Paradise Group's Journey From Acronis to Druva

Paradise Group Holdings Pte Ltd is a Singapore-based restaurant group incorporated in 2002 by Eldwin Chua and Edlan Chua. The company's restaurants serve a variety of Chinese cuisine.

The Challenge

- Paradise Group's on-prem Acronis backup system was limited by storage capacity and lacked off-site backup, posing risks.
- The system consumed valuable server space and had limited compute resources.
- As a Microsoft/Azure-focused company, Paradise Group needed a solution supporting VMware, shared files, and Azure backups.
- They required a future-ready, secure data protection solution to support their growth and public-facing operations.

The Solution

- Paradise Group chose Druva over Veeam and Acronis for a fully managed SaaS platform designed to reduce operational overhead and strengthen cyber resilience.
- Within one week, they migrated VMware, Azure VMs, Microsoft 365, and user files to Druva, benefiting from cloud scalability and resilient off-site backups.
- Druva's cloud-native approach reduced on-premises infrastructure dependency, freeing IT resources for strategic projects and making cloud migration seamless compared to their old solution.

Highlights

- Paradise Group replaced Acronis to solve storage and off-site backup challenges.
- The IT team achieved a 30% reduction in TCO by adopting Druva's cloud-native platform
- A one-week migration process enabled Paradise Group to quickly secure VMware VMs, user files, and Azure instances
- Druva provided the Paradise Group team with a reliable "safety net" and confidence in their cyber resilience

[Read the full customer story ↗](#)

Elmet Consolidates Four Data Protection Vendors & Saves \$40K Annually with Druva

Elmet Technologies is a fully integrated global leader in the production of high purity molybdenum and tungsten products and fabrications. Founded in 1929 and 100% US-owned and operated, Elmet serves a wide array of industries including defense, lighting, electronics, semiconductor, thin film, automotive, aircraft, and medical. With its corporate headquarters and manufacturing site in Lewiston, Maine, Elmet Technologies is ITAR registered, and its production management systems are certified to AS9100 and ISO9001.

The Challenge

- Managing VMware backups was inefficient due to multiple disparate solutions, leading to operational complexity and slow recovery times.
- Lack of a unified platform to protect and manage data across six remote and branch offices (ROBO) globally.
- Ensuring compliance with stringent security standards like FedRAMP was difficult with the existing fragmented backup infrastructure.
- Elmet urgently needs to consolidate and simplify data protection to support manufacturing operations.

The Solution

- Druva provided seamless integration with VMware, enabling standardized, efficient backup and recovery for enterprise workloads.
- Druva's cloud-native platform centralized backup management for all six ROBO sites, simplifying operations and improving visibility.
- Druva's FedRAMP certification ensured Elmet's data protection met required governmental compliance standards, strengthening security and regulatory adherence.

Highlights

- Elmet Technologies saved \$40K annually by consolidating four separate backup solutions into a single, unified platform with Druva.
- Achieved 50% time savings for system admins through streamlined operations.
- Secured comprehensive Microsoft 365 data backup, reducing risk and increasing reliability.
- Leverages Druva's FedRAMP-authorized offering to support stringent compliance needs

[Read the full customer story ↗](#)

Rapid Recovery & Robust Protection of Hybrid Workloads at Betenbough Companies

Betenbough Companies owns several subsidiary companies, including Betenbough Homes. They were founded in 1992 and are based in West Texas.

The Challenge

- Betenbough Companies used outdated tape backup systems with Backup Exec, Symantec, and Azure tools that were inefficient.
- System slowness and inability to handle rapidly growing data effectively was a major challenge.
- Manual monitoring and troubleshooting processes were time-consuming, taking hours each day.
- Occasional minor data loss incidents occurred, underscoring the need for a modern cloud-based data security solution.

The Solution

- After a ransomware attack impacting hybrid workloads, Druva's disaster recovery enabled Betenbough to restore critical systems within 24 hours.
- Druva streamlined backup and recovery for 114 TB of data across Azure VMs, VMware VMs, Windows, NAS, and SQL environments.
- Betenbough later expanded Druva usage to cover Microsoft 365 and Azure VMs, enhancing data security and ransomware protection.

Highlights

- Recovered from a ransomware attack in just 24 hours with Druva's DRaaS solution!
- 114 TB of data protected across various platforms including Azure, VMware, Windows, NAS, and SQL.
- 5x global deduplication storage savings

[Read the full customer story ↗](#)

How Druva Delivers Radical Simplicity

Druva delivers a radically simplified approach to protecting and managing data across diverse environments. Built as a fully managed SaaS platform, Druva reduces backup complexity and strengthens cyber resilience with ransomware detection, verified clean recovery, and immutable and air-gapped backups.

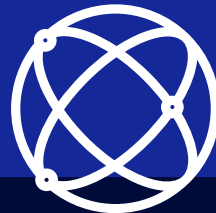
- **Direct-to-Cloud SaaS:** Deploy in minutes with a fully managed SaaS platform—without deploying and maintaining backup servers or storage systems.
- **Always-Immutable Backups:** Backups are air-gapped and encrypted (AES-256), isolated from primary environments to thwart ransomware and insider threats.
- **AI-Driven Intelligence:** DruAI automates the restore process, guiding investigation and policy validation through intelligent agents.
- **Optimized Performance:** Global source-side deduplication reduces bandwidth usage by up to 80%
- **Local Recovery Flexibility:** LAN-speed local recovery for select workloads without infrastructure sprawl.



- **40% TCO Reduction:** Lower costs by reducing infrastructure and utilizing consumption-based pricing with no egress charges.
- **Zero-Trust Architecture:** Built on role-based access control (RBAC) and certified with SOC-2 Type II, HIPAA, and FedRAMP.
- **The \$10 Million Guarantee:** Peace of mind from the only vendor to back data protection against common risks with a multi-million dollar guarantee.

Advanced Security & Recovery Capabilities

- **Managed Data Detection & Response (MDDR):** 24/7 monitoring with "Safe Mode" to lock down environments during a suspected breach.
- **Threat Insights:** Stop threats before they strike with the continuous scanning using Threat Insights, then investigate and neutralize attacks instantly with Threat Hunting.
- **Disaster Recovery (DR) Orchestration:** One-click failover into customer VPCs or across regions with automated runbook orchestration.
- **Unified Observability:** A single console provides real-time insights into backup security and actionable alerts for unusual data activity.



Next Steps

The combination of hybrid sprawl and targeted ransomware has made legacy "do-it-yourself" models a liability. As we look toward, the measure of a successful IT leader won't be how much hardware they manage, but how quickly and cleanly they can recover.

Take Action Now!

Ready to stop managing infrastructure and start managing resilience?

- Data Center Backup ([VMware Protection Product Tour](#))
- Flexible, local recovery with TurboTier [Product Tour](#)
- Get a 30-Day [FREE Trial](#)



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](#).