



powered by  aws

Protect data anywhere with Druva and AWS

Data explosion creates new backup challenges

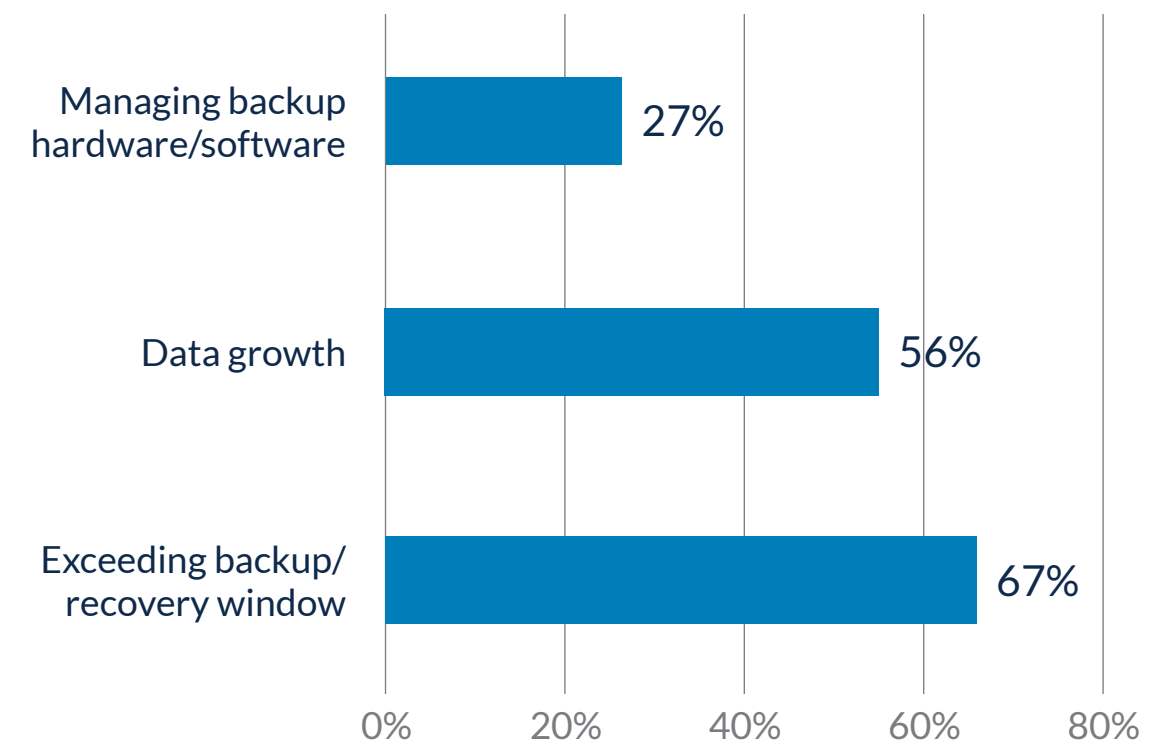
The incredible explosion of data has opened the door to new challenges for data protection, which are identified by IT managers and admins in a recent 451 Research report:

- Managing backup hardware/software associated with their current solution
- Rapid growth of unstructured data
- The inability to back up all data within a specific window

Data Protection for the Cloud Era

Working together, Amazon Web Services (AWS) and Druva eliminate these pain points with cloud-based data protection. Built on top of AWS' highly available services, Druva delivers global backup and disaster recovery, all managed by a unified management console. Druva offers off-site immutable data copies that reduce backup operating costs and act as your last line of defense against ransomware.

Top backup pains



Source 451 Research's TheInfoPro Storage Study — Wave 18

Innovation that **eliminates pain points**

“With limited IT staff, Druva helps us remove the tedious tasks of daily hardware management, frees our IT staff for more application related tasks and helps drive focus on business intelligence.”

**Chris Fernon, Director of Enterprise Technology
GameStop**

Zero hardware

Druva's SaaS platform eliminates dependence on hardware, software and the never-ending refresh/upgrade cycles associated with their maintenance. Druva is easy to use with single-click workflow automation that backs up and fails over your data into the cloud. You can also replicate backups across multiple AWS regions and accounts for an added layer of protection.

50% lower TCO

Global source deduplication reduces the amount of data needed to be protected by 3-5X, the impact of which can be seen in the reduction of network congestion, faster backups and reduced storage costs. Druva's intelligent long-term data retention transparently moves data for business, legal and compliance purposes into Amazon S3 Glacier Deep Archive to further reduce overall storage costs.

Unified management

Druva delivers a single user experience to protect data across data centers, NAS storage, endpoints, SaaS applications and AWS infrastructure and databases. Its unified management console simplifies data protection.

Modernize your data protection with these use cases:



Simplified cloud backup



One-click disaster recovery and failback



Protect AWS workloads



Metadata file search, governance and compliance



Automating data retention

Simplified cloud backup

Ditch backup hardware and software. Druva's solution is easy to implement and provides instant access to your data.

Backup options include:

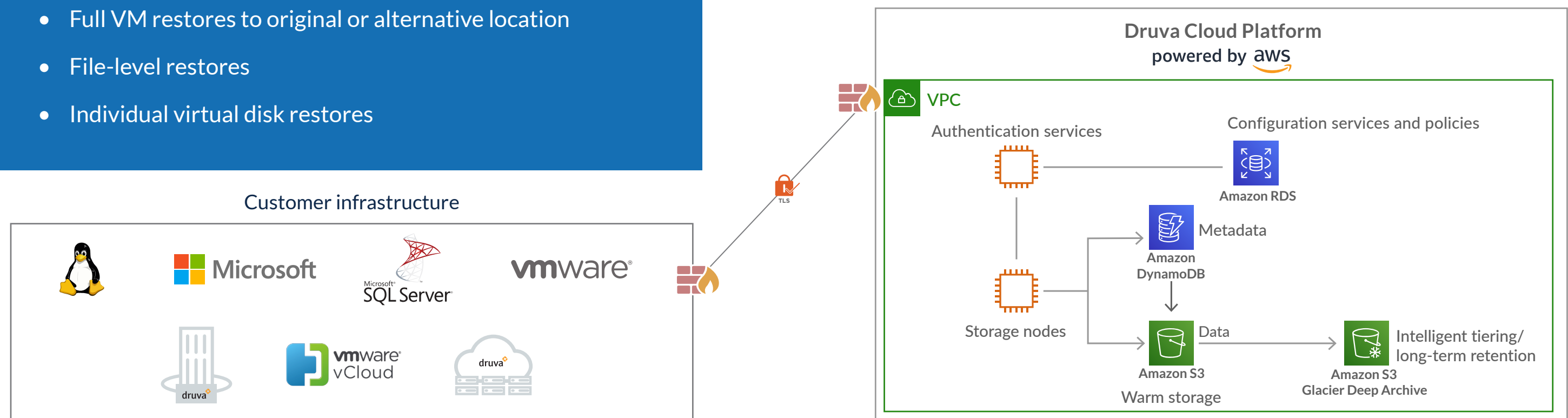
- File level backups
- Application aware backups (VMware and MS SQL)

Data restore options include:

- Full VM restores to original or alternative location
- File-level restores
- Individual virtual disk restores

How it works:

- An agentless proxy is installed into your on-premises infrastructure
- Identify new data blocks, complete dedupe hash lookup
- Encrypt and transmit new data blocks to Druva Cloud Platform
- Data and metadata are stored separately to obscure data path
- After 15 days, data designed for long-term retention is transparently moved to Amazon S3 Glacier Deep Archive
- Replicate backups across AWS regions and accounts



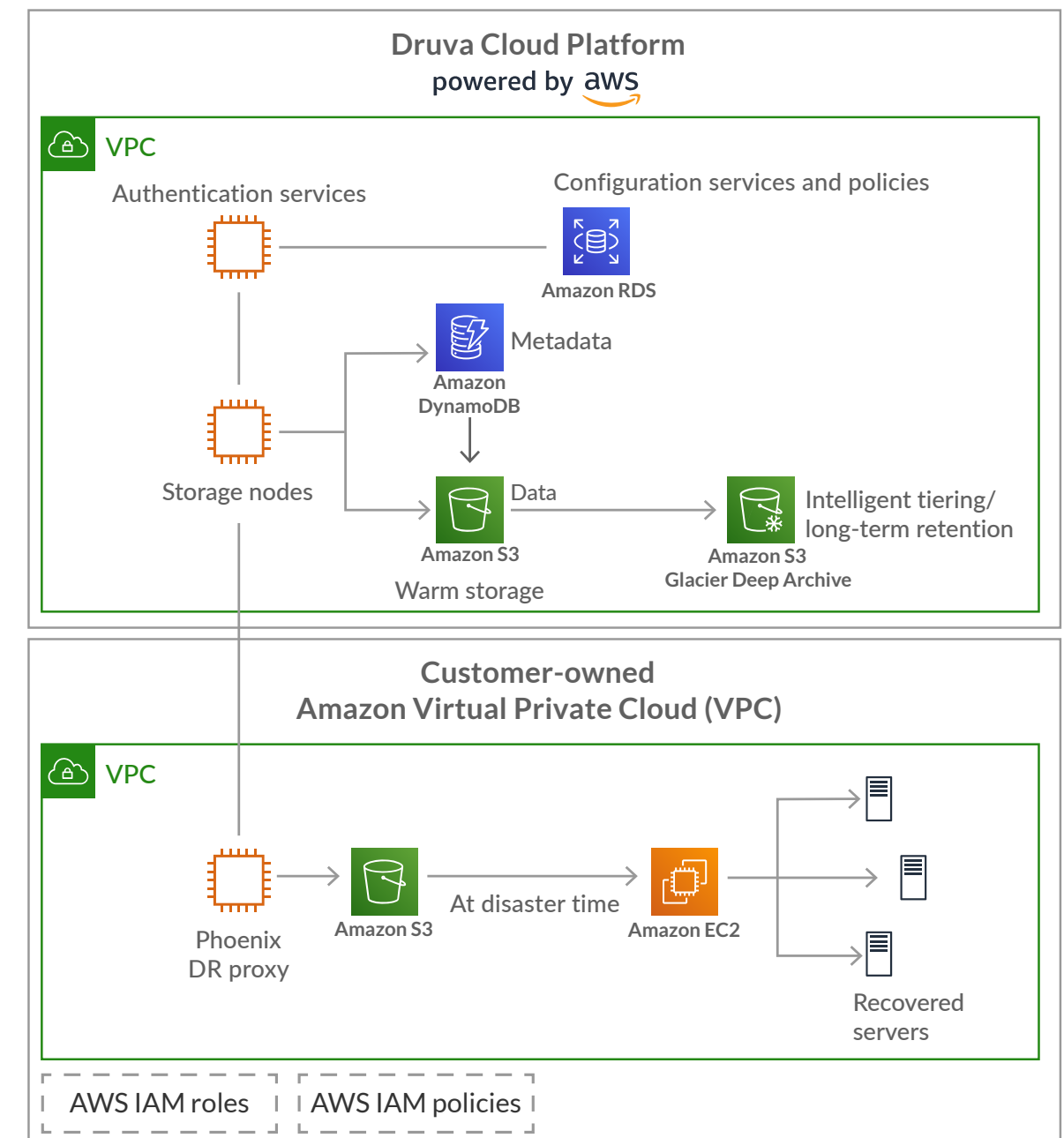
One-click disaster recovery & failback

Maintain business continuity with automated failover to keep your business running when unplanned downtime or a cyber villain strikes.

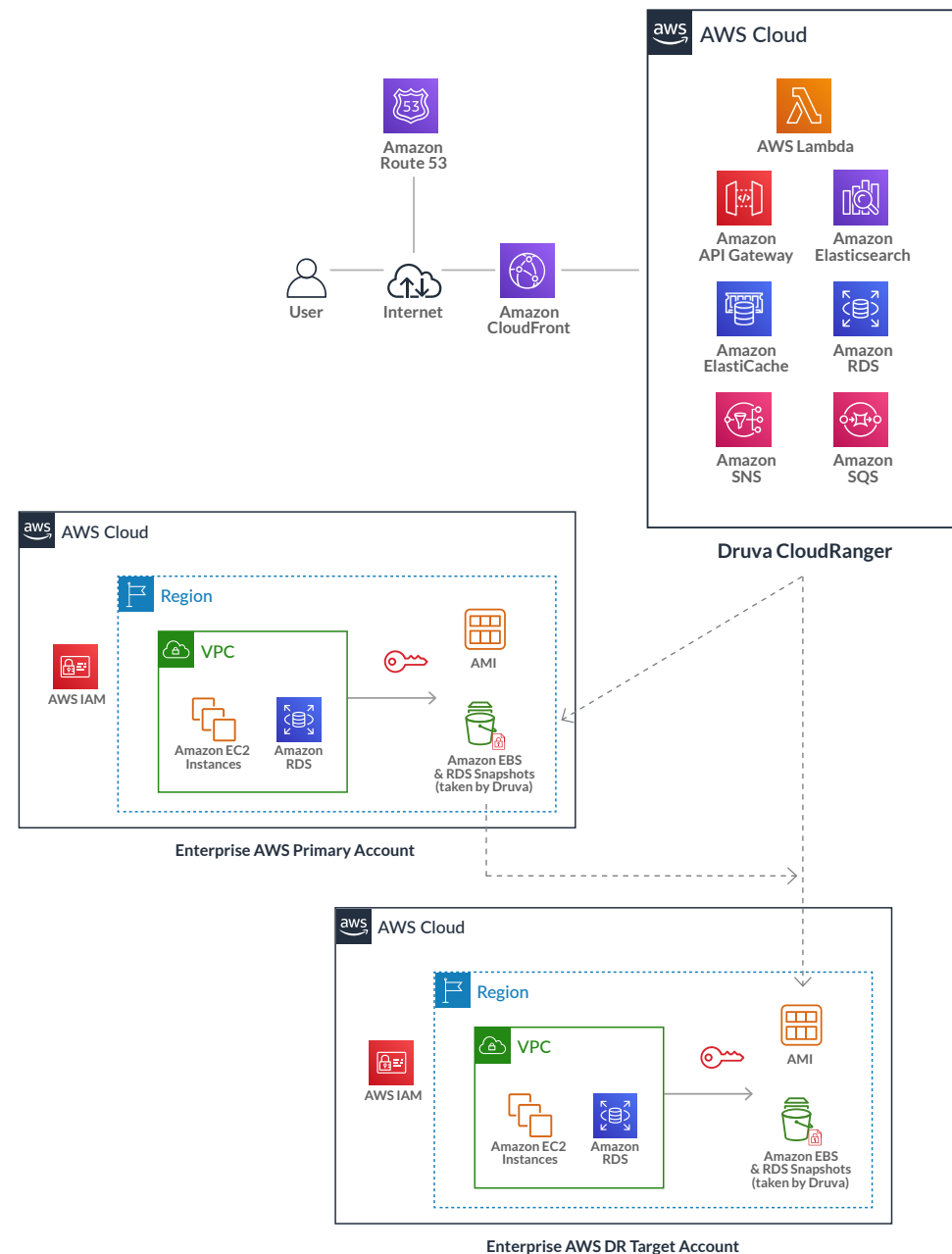
Here's how to prepare:

1. Provision your own Amazon Virtual Private Cloud (Amazon VPC). Using AWS CloudFormation template(s), install the Druva proxy to create IAM roles and policies and replicate your backup copies in the Amazon VPC.
2. Create a disaster recovery (DR) plan using the built-in templates to configure both production failover and DR test settings, including:
 - Amazon VPC details
 - Network & security groups
 - Virtual machine (VM) boot sequence
3. Automation and orchestration lets you precheck and test your DR plan. Make the appropriate adjustments identified by the test.

At the first sign of unplanned down time, a single click initiates your DR plan to recover virtual machines in approximately 15 minutes. After the disaster is mitigated, failback your data to the production environment.



Protect AWS workloads



Backup and recovery

What it does:

- Global backup policies across AWS infrastructure for AWS cloud and AWS GovCloud

What you can do:

- Set up global backup policies and custom schedules for Amazon EC2, Amazon EBS and Amazon S3
- Back up Amazon S3 buckets and objects then archive Amazon EBS snapshots to Amazon S3
- Instant recovery of volume, files and virtual instances

Disaster recovery

What it does:

- One-click disaster recovery and scheduled DR tests to validate RTO/RPO compliance

What you can do:

- Create cross-region/account DR plans for Amazon EC2 and Amazon RDS
- Clone environments with region-based mappings

Metadata file search, governance, and compliance

Metadata file search:

- Scan and index snapshot files
- Search snapshot file systems
- Find point-in-time files
- Search snapshot file systems

Governance and compliance:

- Automated compliance reporting
- Granular search to identify files and data
- Role based Identity Access Management
- Data never leaves your cloud

Federated Search File Search Email Search

Q Enter file name or SHA1 hash value ☐ Match Exact Words

File Extension ▼ Data Source ▼

File Size From To

Time Modified From To

Time Created From To





Profiles ▼

Users

Reset Search

File Violations Active Resolved Quarantined

Resolve Download Showing 200 Violations Search by Username or Email ≡

<input type="checkbox"/> File Name	Modified On ↑	User	Sensitive Data Matched	Policy Violated
<input checked="" type="checkbox"/>  Group Mediclaim Policy...	Jun 12 2018, 10:50	Ernie Carter	 Employee Identification...	Some Policy Name +1
<input type="checkbox"/>  Lab Tests.docx	 Jun 12 2018, 10:50	Katayama Fumiki	Social Security Number, +2	Another Policy Name

Automating data retention

IT managers and admins identify establishing data retention policies as one of their top five data protection pain points. IDC estimates that approximately 60% of all corporate data is cold, 30% warm, and 10% is hot. But while cost reductions can be experienced by storing 60% of your data on a different storage tier, moving this data manually is labor-intensive.

Druva's intelligent automation reduces storage costs by automating the tiering of data from Amazon S3 to Amazon S3 Glacier Deep Archive, providing a cost-efficient long-term retention solution.

IDC, 2019

Benefits:

- Increase operational efficiency using a single template to configure both backup and data retention policies
- Reduce hidden costs and complexity by eliminating data egress charges from cold to warm storage
- Single fixed price for global storage vs. data retention in customer-owned AWS account(s)
- Easier access to data for business analytics vs. tape systems
- Access enhanced business insights with global search that includes data retained for compliance and eDiscovery

Create New Backup Policy: VMware

Summary Backup Schedule Retention VMware Settings

Retain

Daily Snapshots for 14 Days Monthly Snapshots for 3 Months

Weekly Snapshots for 4 Weeks Yearly Snapshots for 3 Years

☒ Enable Long Term Retention (LTR) ⓘ

Eligible snapshots will be moved to cold tier after 15 days.

Cold Snapshots will take longer to restore. The data needs to be restored from cold tier to warm S3 tier, which typically takes upto 36 hours.

If the cold snapshots are deleted before the minimum LTR retention period, early delete fee will be applicable.

Previous Next

Enabling long-term retention is a simple click while setting up backup policies

Next steps

Learn more about the Druva
and AWS partnership

Discover Druva — AWS
solutions

Tuesday Live!
Schedule live demo



Find Druva in AWS Marketplace

Get Started



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: +81-3-6890-8667
Singapore: +65 3158-4985
Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit [Druva](https://druva.com) and follow us [@druvainc](https://twitter.com/druvainc).

powered by  **aws**