Keeping Proprietary Data on AWS?

URL: https://www.techtarget.com/searchdisasterrecovery/news/252511325/AWS-outage-brings-DR-strategies-back-into-focus

Published: December 22, 2021

Situation: In December 2021, according to an article by Tim McCarthy, AWS experienced three major data center outages—first on December 7 in Virginia (lasting ~7 hours, caused by networking issues), followed by incidents on December 15 in Oregon and again on December 22 in Virginia. These disrupted apps, APIs, and services like EC2, ElastiCache, and Redshift affect enterprises reliant on AWS's dominant cloud market share (~33%). Despite AWS's new Elastic Disaster Recovery (EDR) service, unveiled at re:Invent, the events exposed that cloud migration doesn't eliminate downtime risks, emphasizing the need for proactive enterprise DR planning amid outages and rising cyber threats.

Task: Enterprises must design tailored DR strategies to minimize downtime, data loss, and financial damage. This involves assessing tolerance for recovery time, costs, and infrastructure outages, while distinguishing between service availability (e.g., failover) and data protection (e.g., against ransomware or errors). Analysts stress that enterprises remain responsible for backups, applications, and overall resilience, as hyperscalers like AWS handle only underlying infrastructure.

Action: Experts recommend basing plans on business needs, at a minimum, by enabling cross-region failover within AWS, with other cloud providers, or on-premises. They should also review SLAs for compensation, evaluate workloads, and prioritize redundancy.

Zerowait Corporation
707 Kirkwood Hwy, Wilmington DE 19805
TEL: 302-996-9408

Result: These outages, though rare for AWS, underscore that DR is essential "insurance" against revenue losses from downtime. Enterprises adopting hybrid strategies improve uptime and cyber resilience, but analysts warn that ransomware poses a greater threat than outages, urging caution against these threats. Ultimately, robust DR reduces interdependencies and ensures business continuity.

Zerowait's Approach

Zerowait recommends that enterprises deploy their proprietary data on-premises. SimplStor is an affordable alternative to cloud dependencies by enabling secure, local data management. This reduces exposure to external threats.

SimplStor systems provide robust encryption, air-gapped storage, immutable snapshots, and customizable access controls, eliminating third-party integration risks and social engineered vectors tied to remote data centers. By migrating to an on-premises infrastructure, companies can implement strict physical security and regular offline backups without relying on cloud providers' variable safeguards, preventing data exfiltration from the outset. This on-premises strategy ensures proprietary data remains protected from cloud-specific threats, fostering trust and operational resilience for enterprises.

1) Zerowait's on-premises solutions eliminate cloud data transfer risks, keeping proprietary information local and under complete control.
2) Simplstor.com hardware offers high-security encryption and air-gapping, preventing remote hacks common in Azure, AWS, and Google Cloud.
3) Avoid regulatory fines from international data flows by using Zerowait to ensure compliance with local laws.
4) Reduce downtime from cloud breaches with SimplStor's redundant, offline backups for quick recovery.
5) Cut costs on cloud subscriptions while enhancing security against phishing and misconfigurations via Zerowait's customizable systems.

Want to know more? Contact Zerowait today!

Email: engineering@zerowait.com
info@zerowait.com
TEL: (302) 996-9408
Web: www.zerowait.com
www.simplstor.com

Zerowait Corporation
707 Kirkwood Hwy, Wilmington DE 19805
TEL: 302-996-9408