Storage Quarterly Q1

A snapshot of our department's latest news, insights and resources

Welcome to the inaugural edition of Storage Quarterly, the newsletter dedicated to data storage at ___. We'll demystify complex processes and concepts, share best practices for using your storage, and provide insight into how the Storage product line helps make ___ one of the world's leading firms. In this issue we'll cover all there is to know about **immutable storage**: what it is, how it works, and why it's such an important aspect of data protection and retention.

A data loss disaster

On January 31, 2017, GitLab.com, a popular platform used by developers to develop and share code, went down. Because the company posted a public postmortem, we have incredible detail into the damage: in addition to GitLab.com being unavailable for 18 hours, 5,000 projects, 5,000 comments, and 700 new user accounts were lost permanently.

What was the cause of such a disastrous data loss event? According to the company, the cause was all too relatable for anyone who's ever used a computer: user error. While trying to resynchronize a secondary backup database, an engineer accidentally deleted critical data from their primary database server, thinking it was the secondary. Because the backup database hadn't been syncing with the primary, 300 GB of newly created data were lost.

"Internal actors [are] responsible for 43% of data loss, half of which is intentional, half accidental." - *McAfee study*

The GitLab.com outage was a prominent example of a common situation in data management. Human error often leads to employees deleting data. Attacks by malicious actors, whether internal or external, who erase or modify critical storage are becoming more frequent. Government watchdogs are increasingly requiring lengthy paper trails for financial data. Fortunately for data protection architects, there's a technology designed to ensure your most critical information is safe from deletion, tampering, and corruption: immutable storage.

The principle behind immutability is simple: you create a record, and once immutability is enabled, that record can't be changed. With true immutable storage, no one can modify the record, whether it be a block, an object or a file In the case of GitLab, immutability would have prevented all those critical files from being deleted.

Continue to the Engineers Channel to learn how immutable storage works, and the immutable offerings we have at ___.

A data hostage situation

The IT staff at Danish shipping giant A.P. Møller-Maersk knew this was not a normal outage. In June 2017, systems at offices all over the world were going down thanks to a sophisticated bug planted by attackers. Terminals at 17 shipping ports, responsible for managing the loading and unloading of cargo on Maersk's ships, were made unusable. Their domain controllers, the servers that manage user authentication, authorization, and security for a network, were down as well, impeding recovery efforts.

```
Ooops, your important file are encrypted.

If you see this text, then your files are no longer accessible,
because they have been encrypted. Perhaps you are busy looking for
a way to recover your files, but don't waste your time. Nobody can
recover your files without our subscription service.
```

The "ransom note" sent to infected Maersk terminals

Across the globe, terminals began displaying prompts demanding payment in exchange for the files being made accessible again. It was soon obvious that Maersk was the victim of a ransomware attack.

Continue reading to see how immutable backups can keep your data safe from cyberattacks.

What you should do

Here's some tips for how best to use immutable storage:

- With a variety of low-cost, long-term storage offerings, object storage is ideal for archiving data. If you're storing data to adhere to ___ or government regulations, enable Object Lock for on-premises object or Object Lock for Amazon S3 to ensure your storage is truly compliant.
- If your workload consists of data that production applications require to function properly, create a backup plan with AWS Backup.
- After you set immutability, your data can't be deleted. You will be paying for it, whether you need it or not, until the retention period ends. Storage recommends setting for only as long as you need at the moment; you can always extend the retention period if needed.

Looking for more?

- J.P. Morgan has a guide to protecting against ransomware attacks.
- Read about Gliffy, a small startup that, similar to GitLab, deleted it's *entire* production database by accident. Immutable backups would have come in handy.
- The architects at AWS created a detailed solution for a centralized data protection plan across storage, compute, and database functions.
- A complete report by Columbia University on the cyberattack that crippled Maersk.