Why Backup
Office 365

Datasheet

Perception Vs Reality
Microsoft 365

Instant data is Professionals first preference after persistent connection. The latest digital access trend has converted Everything in IT as a Service .The fact that data, emails, calendars, spreadsheets, presentations and records are now always in the cloud brings ease and convenience at the work place, But how do you ensure your data is safe? Are you presuming or consuming?

In reality even while being on Microsoft Platform you are not guaranteed to be 100% protected and safe. However your data is always residing in the state of the art data center. Many security-related matters still need to be managed by the end users and corporate system administrators.
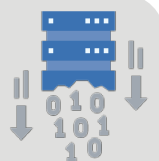
As we've already mentioned, the main misbelief about Microsoft 365 services is that the company manages both the security of your data and its availability. However, it's not that simple.

Microsoft says: "We recommend that you regularly backup your content and Data that you store on the services or store using Third-Party Apps and Services."

As stated in the official Services Agreement, the company ensures the physical security of your data and its automatic replication, provides you with instruments for identity and access management, and ensures service availability (although, according to the terms and conditions, the services might be unavailable" from time to time").

IDC

The threats to data are increasing and the consequences are becoming more serious. Attacks from bad actors have become nearly ubiquitous.

G2

G2 says: SaaS backup software must be able to integrate with other data backup, protection, and/or management solutions.

Why You Should
BACK UP Microsoft 365

The Key reasons you shouldn't close your eyes when it comes to backing up Microsoft 365

#1. To prevent data loss.

Be it Incidental or Accidental but the threat of data loss is always lurking round the corner. Irrespective of Applications hosted hosted and managed by reputed vendors but there is no guarantee of data protection.

First of all, data backup will protect you from accidental and malicious intent. Be it your SharePoint or email data there is threat of Intentional or Accidental data deletion, your important data shouldn't be left without back up Once deleted, gone for ever. This could be lost of email chains, spreadsheets, and other critical data posing numerous financial loss to the company.

Organizations adopting SaaS platforms like Office 365, GSuite, Salesforce, Box and Drop-box, to avail the benefits of its flexibility, scalability and cross platform collaboration. While They are extremely secure solutions, they cannot protect you from data loss at your end - from some of the most prevalent causes, mentioned below ;-
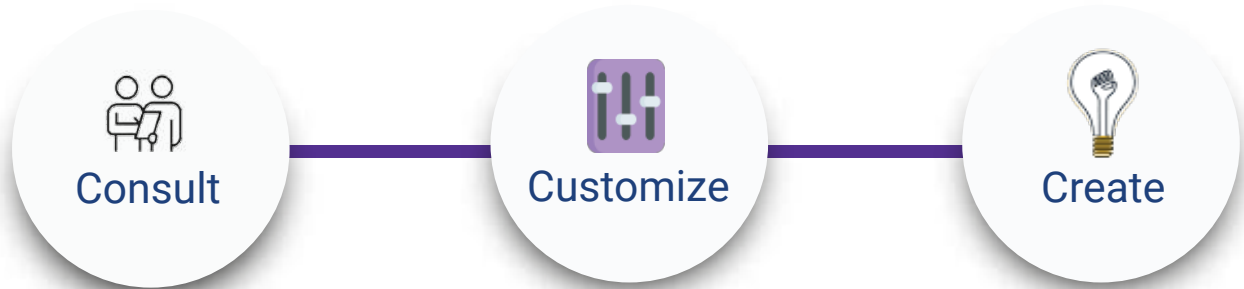
To Err is human

Out Of Sync

Malicious program / intent

Breakdown / Outages

Security Threads Such As Hackers, Malware, Ransomware, Cryptomining, Phishing, Etc

Consult — **Customize** — **Create**

#2. Constrained native recovery and reten-

Microsoft's own recovery solution won't allow you point- in-time recovery of mailbox items. However a full blown backup solution will allow you to back up and recover your data according to your own need and schedule.

#3. Limited regulatory compliance.

Many businesses demands to meet Industry specific compliances, such as HIPAA or GDPR, to name but a few examples. To meet such compliances you need to take extreme care to ensure archival and retention, which could further be purged on demand.
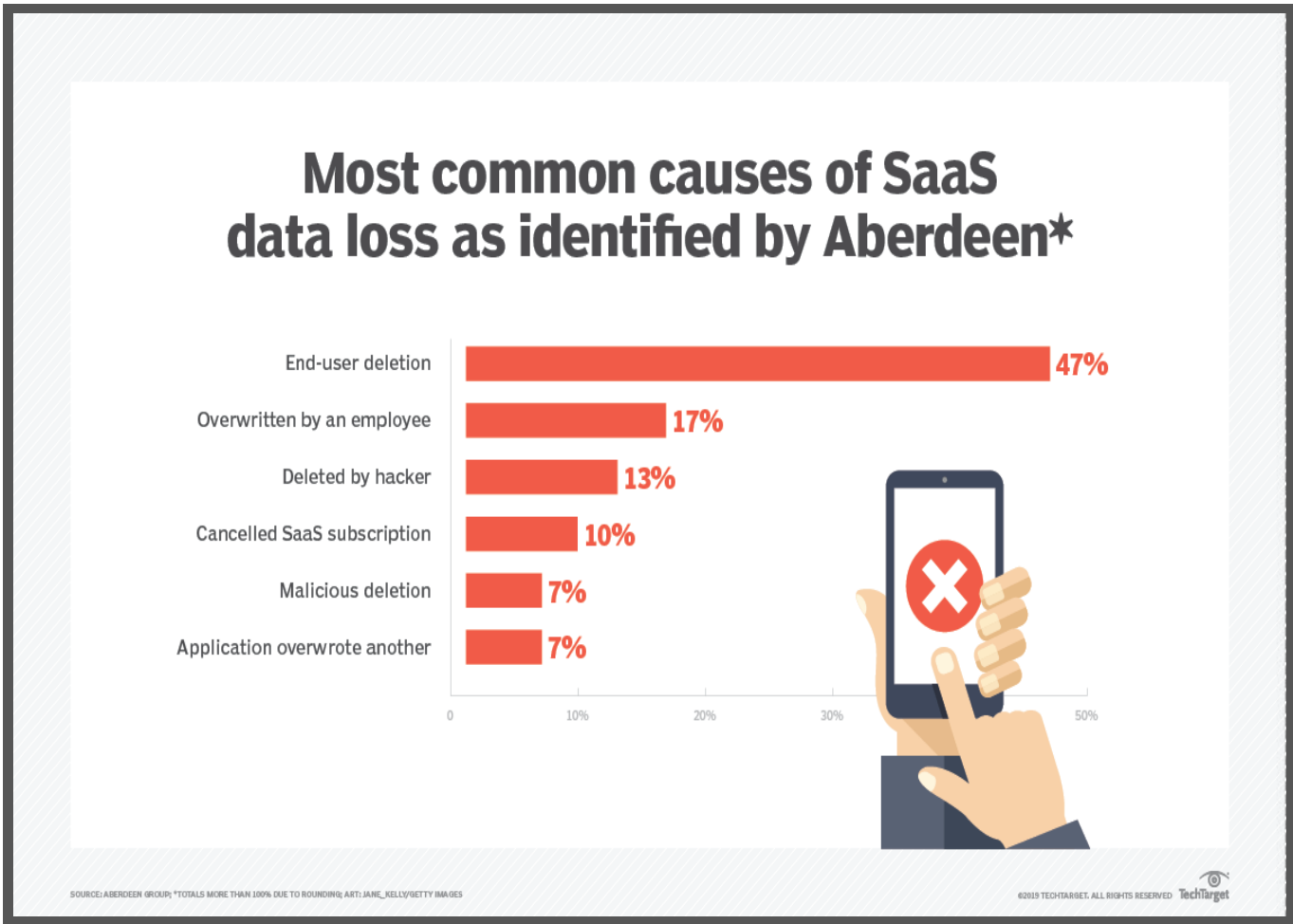
#4. Managing dormant email accounts.

You are still indecisive over dormant account, as you have 2 options to either archive their data and pay for the unused account, or back up all their data to low-cost storage and delete the account. Which one is your choice?

#5. Accessing data in the event of service outages.

However impeccable but, data outages still happen with Microsoft services. Moreover, referring to recent reports, outages have been happening more often in recent years at Microsoft. A customized backup solution will help you to at least access the data that you need in the event of an unforeseen issue with the service.

The Aberdeen Group study found approximately 20% of all SaaS data loss could be attributed a combination of hackers and general malicious activity. Others attributed data loss to ending a SaaS subscription

Most common causes of SaaS data loss as identified by Aberdeen*

Cause	Percentage
End-user deletion	47%
Overwritten by an employee	17%
Deleted by hacker	13%
Cancelled SaaS subscription	10%
Malicious deletion	7%
Application overwrote another	7%

SOURCE: ABERDEEN GROUP; *TOTALS MORE THAN 100% DUE TO ROUNDING; ART: JANE_KELLY/GETTY IMAGES

©2019 TECHTARGET. ALL RIGHTS RESERVED TechTarget

*Logos Copyrights Belongs To Their Respective Owners