CLOUDALLY
Secure Cloud Backup

3

eBook

Guaranteed Remote Productivity Using Cloud Backup

3 Imperatives Guidelines for Improved Disaster Recovery & Business Continuity, in the Work-From-Home Era

Practical pointers to secure your remote workforce and protect business-critical SaaS data

Introduction

Murray Moceri,
Partner Account Director,
CloudAlly

The increase in the remote workforce is not a passing phase. Based on a recent Gartner report, three out of four organizations intend to permanently shift some employees to remote work[1]. Win-win for both sides.

Employees save on transport time and costs while enjoying a more flexible work-life balance. Employers benefit too - reduced on-premise technology spend, lower real-estate and office maintenance expenses, and estimated costs savings of $11,000 per half-time tele-commuter per year[2]. These savings can help organizations struggling with the economic repercussions of the lockdown.

How Do We Provide a Safe & Secure Remote Workforce Environment?

However, this tectonic shift to work-from-home comes with a separate set of security vulnerabilities. Employees with their guard down working on unsecured devices - the risks abound. And the hackers seem to be well-prepared to exploit them. McAfee found that external attacks on cloud accounts grew by a whopping 630 percent from January to April 2020[3].

A breach, especially this year, is something we can all ill-afford. So, how does an organization gone remote prepare for a breach? By adapting its disaster recovery and business continuity processes to remote use case scenarios. This enables the business to retain its capability to recover quickly from possible breaches and minimize their impact. In this ebook we focus on ways the organization's can weather and rebound from a cyber-attack or a data breach with a large remote workforce. Read on for practical pointers and examples for responsive disaster recovery and seamless business continuity.

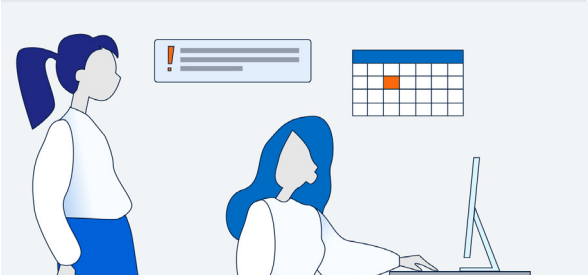
[1] https://www.gartner.com/2020-04-03-gartner-cfo-survey
[2] https://globalworkplaceanalytics.com/global-workplace-analytics-in-the-news
[3] https://www.cnbctv18.com/mcafee-shows-rise-in-cyberattacks-as-cloudservices-use-goes-up-covid.htm

#1 Evaluate and mitigate the security risks of remote work

Analyze all the touch-points, devices and applications used by your remote employees. With reduced security on the employees' personal and/or mobile devices, the vulnerabilities increase. Identify and implement preventive fixes. Some suggestions:

Secure your endpoints

Mandate access only on official devices that are secured with physical and electronic layers of security. Remind employees to regularly update their antivirus and security software - endpoint security is vital. Evaluate installing unified Mobile Device Management (MDM) and Mobile Application Management (MAM) tools.



Work and personal don't mix!

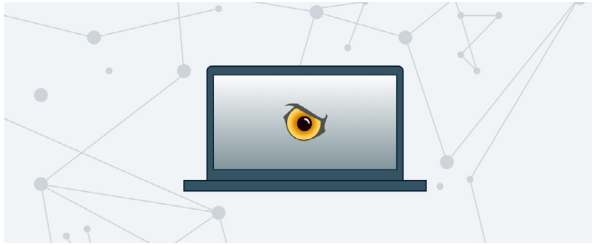
Advise employees to not use their official devices for personal reasons. When personal and business data is mixed the risks increase significantly. For instance, if non-approved software or a pirated movie is downloaded for personal use and the laptop crashes, business data would be lost too.

Train your remote workers to be cyber-secure

Employees can either be your first line of defense or your weakest link as far as cybersecurity goes. It is well-worth investing in nurturing a “cyber-secure employee”.

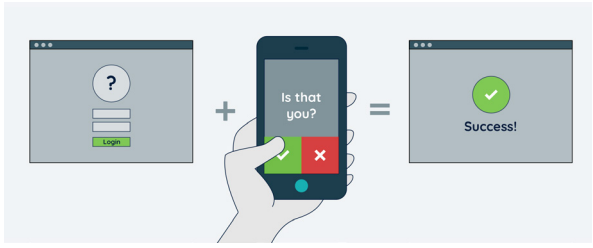
Develop and evangelize a remote workforce policy with employees. Send regular emails publicizing the approved list of software, incident response steps, and upcoming antivirus updates.

Train employees about various social engineering red flags and phishing scams, especially those related to Covid. Encourage them to report suspicious emails and familiarize them with disaster response steps should they become the victim of a malware scam or lose a company device.



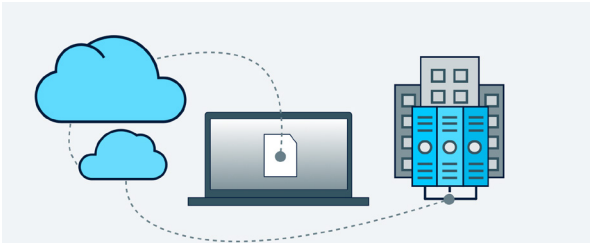
Hawk-eye on the network

Monitor all network requests applying the zero-trust paradigm. If not employing a VPN, avoid opening remote access ports. And if using a VPN, given the recent host of **VPN vulnerabilities,** ensure that it is regularly updated.



Nothing beats MFA/TFA

Above all, ensure that all applications implement **Multi-Factor/Two-Factor Authentication (MFA/TFA)** which can successfully block breaches caused due to compromised credentials; the cause of the vast majority of breaches.



Harness the cloud's scalability and collaborative mechanisms

If you haven't already, strongly consider using cloud computing platforms like Microsoft 365, G Suite, Salesforce, Dropbox. Microsoft Teams is offering it's paid version **free for the next six months**. The cloud offers an inherently scalable and collaborative platform where data remains on the cloud instead of being stored on local devices.

Zero trust is a reliable way to stay secure

Security experts vouch for "Zero trust", a methodology for improved IT network security that is **gaining credence**, particularly with increased remote usage. It basically requires you to assume zero trust for all access requests and only grant access when verified. To do that data has to be gathered and intelligence has to be added to network security engines to make informed decisions on the veracity of the connection request.

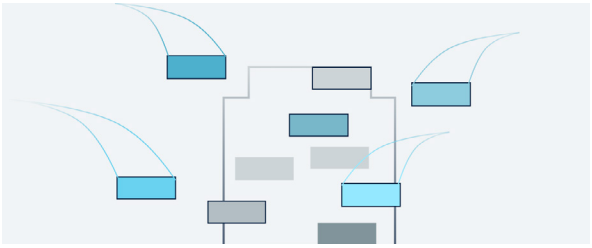
> "One of the best things you can do to prevent attacks is to just turn on MFA. MFA can prevent over 99.9 percent of account compromise attacks."[4]
>
> Melanie Maynes,
> Senior Product Marketing Manager,
> **Microsoft Security**
>
> Microsoft 365

[4] https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

#2 Re-evaluate your Business Continuity and Disaster Recovery Plan (BC/DR)

Whose hand would you reach out for if a security breach were to strike?

Your BC/DR's comforting one, of course! Disaster recovery and business continuity planning are essential processes that help organizations prepare for and recover from disruptions of all sorts - a power outage, platform downtime, phishing attack, credential breach, and others. For the BCDR to stay relevant and consequently helpful, you would need to update it with the can of disruptions that remote-first work have opened. Pointers to kickstart your effort:



Revise Your Recovery Objectives

Your recovery objectives will determine if your disaster recovery is a success or not. The two main markers are the:

- Recovery Time Objective (RTO): The RTO measures your downtime bandwidth - the amount your systems, workflows and business can withstand without incurring damaging losses. Knowing the RTO helps you determine the recovery strategies, processes and tools to successfully recover from a disaster.
- Recovery Point Objectives (RPO): The RPO determines the amount of data loss that your organization can tolerate before tanking. Your RPO will dictate your backup plan, frequency and the supporting infrastructure.

They work in tandem: the RTO tells you how much time you have to get back on your feet and the RPO whether the data you've recovered is sufficient/accurate enough to get you up and running. For example, if you finalize an RTO of 7 hours and disaster strikes at 10am, your services need to be back by 5PM. If your RPO is 10 hours, your backup needs to be scheduled every 10 hours, so that the maximum data loss is 10 hours "worth" of data. Re-evaluate them in view of the remote-first situation where response times of IT teams may be delayed.

Bolster your current BC/DR plan to accommodate for remote risks

A few scenarios that work from home throws up: What is the response time of your now remote IT team? Can your employees self-service recovery? Can I restore data remotely? Where can I store my backups for better accessibility - cloud or on-premises? How quickly can I bulk recover lost data? If an employee loses their laptop how quickly can I delete the data on the lost one and send another?

Assess your current BC/DR plan and see if it can accommodate situations like these and more that are commonplace with remote workforces.

- Perhaps you would need to move from on-premises backup to cloud-based for better accessibility.
- Select a backup solution that supports easy remote recovery and that comprehensively protects all SaaS data with no point-in-time restrictions.
- Train remote emergency response champions/groups in various time zones and inform employees of their contact details.
- Ensure that your recovery software is mobile responsive.
- Evangelize the changes to your BC/DR plan to the various stakeholders and employees.
- Distribute your stock of devices across various locations so they can be transported quickly to employees.
- Run full-scale test drills to check that your BC/DR plan meets the requisite recovery objectives.

"There is a 630% rise in cyber attacks as cloud services use goes up during Covid-19 induced work-from-home."[5]

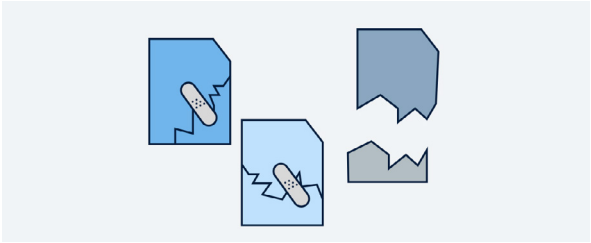
McAfee
McAfee Together is power.

[5] https://www.financialexpress.com/rise-in-cyber-attacks-as-cloud-services-use-goes-up-during-covid-19-induced-work-from-home-mcafee

#3 Centralize your backup in the cloud

With cyber-attacks increasing, and consequently exposing the security vulnerabilities of remote work, data protection is becoming a top business priority. The bedrock of data protection is backup and recovery.

- With the rise in tele-commuting, SaaS-based cloud-to-cloud backup can provide the perfect recoverability, scalability and security that remote backup and recovery demands. Business-critical data and workflows have been migrated to SaaS platforms like Microsoft 365 (formerly Office 365), G Suite, and Salesforce. These are remotely accessed on a host of unsecured devices, in home environments with relaxed cybersecurity constructs. In such a situation, **SaaS platforms need backup**, more than ever, to protect SaaS data from loss due to human error, malicious intent, sync errors, malware, et al.



- Native solutions are archival in nature and not built for data recovery. This means that restore is tedious and destructive (changes are overwritten) without unlimited point-in-time, or cross-user recovery. More importantly, data is only stored for a limited time - from weeks to a couple of months.

- SaaS backup solutions that offer non-destructive point-in-time, or granular restore with unlimited data retention can reduce your RPO and RTO and ensure fast data recovery. Moreover, if they offer self-service restore they minimize the time to recover even further, while reducing strain on IT teams.

- Select comprehensive and centralized SaaS backup solutions that back up data on the cloud thus ensuring your data protection is complete without the risks of on-premises infrastructure issues. For instance, if your backup solution does not include Teams - heavily used by your remote employees - you could risk losing valuable data. Or if your solution backs up data on-premises and there is an outage or your storage is full, you could miss backups till your remote IT teams fix the issues.

> "Back up SaaS data or risk losing customers and partners. Stop leaving the door open to data loss, and start proactively protecting cloud data before it's too late".
>
> **Forrester**

How CloudAlly can help

CloudAlly pioneered SaaS Backup for the enterprise in 2011. Consequently, our backup solutions for Microsoft 365, G Suite, Salesforce, Dropbox, and Box are tried and tested by organizations with thousands of users.

We're top-rated by Gartner Capterra and G2, and were voted as a leading SaaS backup solution by over 10,000 IT Pros in a survey conducted by Newsweek. We're secure, scalable, and built with features tailored to secure the remote enterprise.

Comprehensive Cloud-to-Cloud Backup:

Complete SaaS data protection of Microsoft 365 including Mail, Calendar, Contacts and Tasks, OneDrive, SharePoint, Groups and Teams (heavily used by remote teams). Similarly G Suite backup includes Gmail, Team Drives, Sites, Calendars, Contacts, Tasks, and Metadata backup. Salesforce backup encompasses all your Salesforce data, metadata, Chatter feeds, and Metadata. Box and Dropbox backup includes all data and folders.

Easy Remote Workforce Management:

Simplified employee on-boarding and off-boarding with bulk activation, automated addition/deletion users, and backup of inactive accounts.

SaaS Backup on Amazon AWS Storage:

CloudAlly stores backups on the stringently secure Amazon AWS S3 storage and encrypted using advanced AES-256 bit encryption Backup solutions with on-premises storage cannot provide remote data security, with the same ease and control that SaaS backup can.

OOTB Setup, Zero Adoption Effort:

Seamless integration with all SaaS platforms – Microsoft 365, G Suite, Salesforce, Box and Dropbox, intuitive UI with admin-friendly tools.

Flexible Remote Recovery Options to any Storage with Unlimited Retention:

Self-service, point-in-time, granular, and cross-user restore. Non-destructive with unlimited retention. Backup to your own cloud storage.

High ROI with Unbeatable Pricing:

Custom discounts for bundles, high-volume and multi-year packages. Save on platform license costs with inactive account backup.

Secure and Audit-Ready:

Global data centers, GDPR, HIPAA and SoX compliant, ISO 27001 certified, MFA/2FA, OAuth and OKTA support, AES-256 data encryption, 99.9% uptime SLA.

Tier 1 – 365x24x7 Real-person Customer Support:

Highly-responsive customer service with a multi-channel Customer Support Hub. We're always on-call to resolve your data protection challenges.

> "Due to Covid-19 our venues have been closed to the public since March and therefore we have lost 80% of our revenue. Moving to CloudAlly for Office 365 backups has allowed us to protect our data in a more cost effective manner. Having used CloudAlly previously I knew that the product would work for us and was likely to be more cost effective for us while in this difficult time"
>
> **CloudAlly Customer Feedback**

Contact us Now! | 14 Days Free Trial | Schedule a Demo

www.CloudAlly.com
+1 (424) 304 1959