Enterprise Architecture Technical Brief
End User Services - Enterprise Endpoint Backup

Contents

Enterprise Architecture Technical Brief
End User Services - Enterprise Endpoint Backup

Context

This document will focus on the user end-point backup to a hosting cloud service.
With end user services constantly evolving to address important items such as mobility, BYOD, virtualization and service component standardization, a solution beyond a simple server backup/restore is needed that will manage, protect and govern end-user device data no matter where it is located (on endpoint devices or in the cloud). According to Gartner with more user data residing in the cloud, endpoint backup is gradually morphing from a simple PC backup focus into a more comprehensive, end-user data protection and management platform.[1]

It would be beneficial to maintain, and promote an enterprise endpoint end-user backup standard that focuses on protecting the user's unmanaged data and to promote best practices for selecting a cloud hosting service provider for the endpoint end-user backup service. The vast majority of this type of solution is offered as a software as a service (SaaS).

This strategy does not intend to replace the traditional server backup/restore (a predictable scheduled backup) of mission critical data

Endpoint Backup Definition

Gartner defines endpoint backup as the process of protecting and managing unmanaged data generated by users with unpredictable schedules and locations (Pushan Rinnen, 2015). Today, endpoint is used most commonly in network security and end user mobility circles to mean any device outside the corporate firewall. This could be a laptop, tablet, or mobile device on the "edge" (or periphery) of the network.

Selecting a Cloud Hosting Service for Endpoint End-user Backup

When selecting a hosting service provider for utilizing the cloud as an endpoint backup, it is recommended to make full use of product capabilities where ever possible, including PC migration, mobile device support, and remote wipe. It is highly suggested that agencies thoroughly investigate the native (capabilities offered at no additional charge) backup/recovery capabilities offered by the SaaS provider, in addition to its high-availability (HA) functions and disaster recovery (DR) plans[2]. Agencies should also work closely with VITA when selecting a cloud hosting service to ensure compliance requirements are met.

Gartner predicts that by 2018, 70% of business application owners will have more self-service control over their data protection services (Pushan Rinnen, 2015). The following are best practices (Pushan Rinnen D. R., 2016) when evaluating a cloud hosting service provider for end-user endpoint backup:

- The service should offer centralized protection and management platform for end-user data in the cloud
- The service should protect and manage data across all endpoints (i.e.: laptops, smartphones, tablets)
- The service should have zero impact to end user productivity (tunable resource controls)

---

[1] Rinnen, R. and Rham, Robert (2015, November 12). Critical Capabilities for Enterprise Endpoint Backup. Retrieved from https://www.gartner.com/doc/reprints?id=1-2S5PESA&ct=151112&st=sb

[2] Pushan Rinnen, Dave Russell (2016, June 10). Data Backup/Recovery Factors to Consider When Adopting SaaS. ID: G00273937 Retrieved from https://www.gartner.com/doc/reprints?id=1-3Q6JAUW&ct=170111&st=sb&mkt_tok=eyJpIjoiT1RabFkyRTNObVJrWXpReCIsInQiOiJOOTRlVUtPdDVPZU13c1E5MjNjNUlKMEJDM0xtM05mcGFnOENGbm4yMTFsUXR3cVZxam5YVlJyV2lrekxzYU9wMUUyQWdueStGdG5TT1RxZ3B0VWVjT0lla09obzQ0QmdrTUVBdGJLa1E5eVZnd3BNSlRmaU9OQkdNSEpJek1xeiJ9

- The service should offer unified visibility and search across your data for fast identification for governance issues.

- the service should offer a self-service file backup/recovery capabilities for users
- (Connor, 2016) have" but not mandatory.

- The service should offer appropriate level of encryption (both in-transit and at-rest) and sufficient data security features to ensure compliance with all applicable rules, regulations and agency guidelines.

- The service should have optimal support for the backup and restore issue. If possible, include a full test of the service provider's support process and expertise as part of your evaluation (it's nice to able to speak to a real person when needed). (Connor, 2016).

- Don't assume that high-availability and disaster recovery capabilities offered by service can recover data loss by user errors or malicious attacks.

- Keep in mind that the provider may not be able to recover from all data loss scenarios and/or deliver fast recovery.

In addition, Gartner recommends asking the hosting service provider the following backup/recovery questions in order to fully understand the capabilities of the SaaS provider compared to your internal requirements (Pushan Rinnen D. R., 2016):

- Does the hosting solution offer native backup that can be used to recover from user accidental or malicious deletion and/or overwrites, as well as file corruptions?

- What kind of data is backed up and not backed up? For a SaaS solution that has many components, such as Google Apps, Microsoft Office 365 and Salesforce, make sure to drill down on each component's backup/recovery needs.

- Can the backup data be used to recover from all data loss scenarios such as user deletion (accidental or malicious), overwrites with incorrect data, data corruption, or other problems caused by data migration and third-party application errors?

- Where is the backup data stored? Can customers specify a backup location among SaaS provider data centers? Can customers backup and restore SaaS user data on their own premises?

- How long is the native backup retained? Can customers update the retention period to meet their needs? If so, at what cost (as longer retention periods can consume a large amount of storage)?

- What are data erasure policies when retention expires?

- Can end users and/or customer IT restore their own data from the SaaS native backup?

- What are the granularity levels of restore capabilities by end users, IT, and the SaaS support team?

- Is there a cost associated with a recovery request to the SaaS support team? If so, how much?

- How long would specific recovery scenarios take? Does the SaaS provider offer guidelines and SLAs on restore requests and any guarantees on the amount of time that certain actions or the entire process would take?

Third Party Hosting Service

While evaluating a hosting cloud service for an endpoint backup, you may find the service does not have all the capabilities your agency needs, such as long-term retention and automated backup/recovery. In this case, Gartner recommends a 2nd set of question to ask a third party hosting service for providing the needed capabilities for your endpoint backup solution (Pushan Rinnen D. R., 2016). They are as follows:

- What specific SaaS data can be backed up?
- What data can't be backed up due to API limitations?
- What are the recovery value-add functions that can save time to justify the additional cost, compared to native SaaS functions?
- Are there recovery limitations imposed by SaaS providers when ingesting restored data back to the SaaS location, especially for large restores?
- Can the backup tool scale for large enterprises?
- Where is the backup data stored? Does the customer have the flexibility to store the backup in another cloud data center or their own on-premises data center?
- Can users design their own retention based on their needs? Is there a cost associated with retention period, and if so, how much is it?
- What happens if a vendor folds its business or discontinues the backup product?
- Does the vendor or product protect other data, such as on-premises applications? Decide for yourself before talking to a vendor if SaaS backup is better treated as a stand-alone capability.

Tactical Approach:

The tactical approach to user end-point backup is to follow common best practices[3] (Connor, 2016) for cloud based user end-point backup hosting. This would entail planning; always have a project plan or a formal process to guide you in your evaluation, procurement and implementation in support of your cloud-based backup and restore strategy. Do your best to have a basic understanding of the architecture for hosting, i.e. direct-to-cloud, hybrid with local caching, hybrid with local storage and cloud archiving, testing, encryption, seeding of backups, archiving in the cloud, cloud backup redundancy, and support. VITA's Platform Relationship Office (PRO) can assists your agency in this effort.

Questions for your organization to think about:

Would your agency feel comfortable leaving the majority or all of the backup/restore capabilities in the hands of the SaaS provider and is your agency willing to engage in potentially very manual and error prone recovery processes in case a data loss occurs?

[3] Earl Follis and Deni Connor, B. (2016, November 21). Cloud-Based Backup and Recovery. Retrieved from http://www.ssg-now.com/