Solution Showcase

Total Endpoint and O365 Protection with Carbonite

Date: November 2019 **Authors:** Christophe Bertrand, Senior Analyst; and Monya Keane, Senior Research Analyst

Abstract: Backing up corporate workers' endpoint devices is not optional. Protecting cloud-resident data, email in particular, is also imperative due to heightened cyber risks including regular ransomware events. But many newer cloud-based applications give organizations a false sense of security that their endpoint data is safe and recoverable. Backing up endpoints and protecting the SaaS data employees are generating from those endpoints is where Carbonite can really help.

Introduction: Misconceptions About Endpoint Backup Promote a False Sense of Security

Data protection must encompass all business data, not just server-resident data. These days, workers use endpoint devices not only to generate and store data locally, but also to create cloud-resident data using software-as-a-service (SaaS) applications such as SharePoint and other Microsoft Office365 apps. Endpoint-resident and SaaS-generated data can be highly vulnerable to loss—more vulnerable than information held in the corporate data centers. And beyond that protection-specific issue, organizations must also account for regulatory compliance and risk management:

- Certain regulations now impose fines on companies that fail to properly maintain and protect particular types of sensitive secondary data, including backups of endpoint-generated or endpoint-stored data.
- Ransomware has become a very expensive problem affecting more than just recovery timeframes. Often, a ransomware infection starts with an innocent-looking email that a user opens through an endpoint device.

According to ESG research, one of the top data protection mandates from IT leadership is centered on improving data protection service levels (SLAs) for recovery. That isn't easy. IT decision makers surveyed by ESG say that several technology meta-trends are complicating their organizations' data protection strategies, including cloud computing and cybercrime. In fact, 25% of respondents said they believe cloud computing will be the meta-trend that causes the most disruption in their data protection strategy, and 14% said that they expect cybercrime to be the most disruptive.[1]

The situation gets worse when it comes to endpoints. Some companies employ many remote workers; others enforce bring-your-own-device policies. As a result, business-critical and sensitive data sits on remote devices and/or on devices not even owned by the organization. Fewer respondents (32%) expressed high levels of recoverability confidence in regard

[1] Source: ESG Master Survey Results, *2018 Data Protection Landscape Survey*, November 2018.

to endpoints owned by the organization than for on-prem server-stored data (42%). And the percentage of respondents who are very confident in the recovery of user-owned endpoint devices was the lowest of all, at 29%.[2]

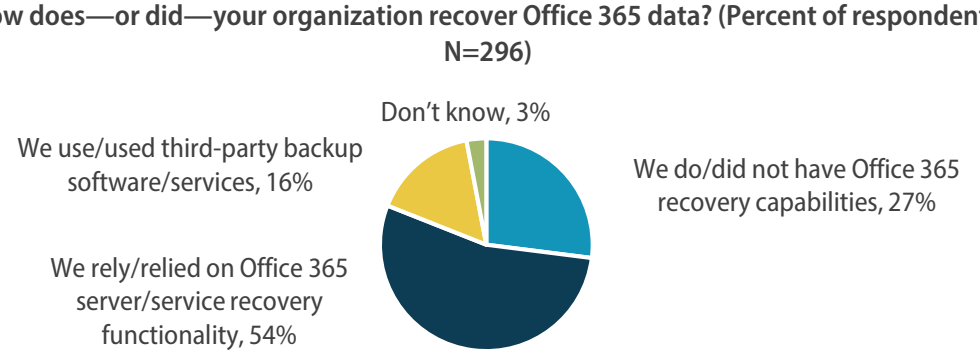
Cyber threats and the other factors mentioned are prompting high levels of concern within some IT departments, but overall, there's much room for improvement in endpoint and O365 backup. Right now, too many organizations still think they don't need to change anything. Those organizations need to remember that not all employees' endpoint devices are formally locked into the corporate network. And not all employees obey company policies that prohibit them from placing or sharing files on platforms (such as Google Drive and Dropbox) that are unsupported and unprotected by IT.

The SaaS Disconnect

A lot of organizations also mistakenly think their SaaS data is backed up by Microsoft or other SaaS platform vendors. Actually, backups remain the organization's responsibility. This misunderstanding reflects the big disconnect related to data protection and SaaS. Consider that 33% of data protection professionals surveyed by ESG believe SaaS-based applications don't need to be backed up, and in the same survey sample, 37% reported that they are relying solely on their SaaS vendor to handle the protection of SaaS-resident application data.[3]

The Office 365 suite of SaaS applications presents a great example of this disconnect when it comes to recovery. As Figure 1 shows, more than one in four ESG survey respondents say they have no O365 recovery capabilities.

Figure 1. The Big Office 365 Backup Disconnect



Source: Enterprise Strategy Group

This finding is particularly troubling because in general, recovery of O365 data can be a bit dicey. Only 21% of respondents who have had to recover O365 data reported they achieved a recovery success rate of 100% (i.e., all data was recovered). Seventy-four percent of organizations that had the best success with O365 data recoveries (more than 75% of data recovered) were using a third-party backup solution instead of built-in tools or nothing at all.[4]

With O365, the stakes are high because the workloads are often mission critical. Ensuring recoverability should be paramount. When choosing a backup solution for SaaS-based applications such as O365, ESG survey respondents are looking for certain features that matter most to their business's productivity. The top three desired capabilities are:

- An ability to restore large data sets from point-in-time snapshots (cited by 25%).
- Advanced protection and recovery of specific applications (24%).
- Data protection SLAs (23%).[5]

[2] ibid.
[3] Source: ESG Master Survey Results, *Data Protection Cloud Strategies*, June 2019.
[4] ibid.
[5] ibid.

Requirements for Successful Endpoint Protection

When it comes to endpoint protection, conversely, the big "must-have" capabilities are a bit different. In ESG's opinion, based largely on IT end-user feedback, the following requirements are crucial to establishing successful endpoint data protection:

- The solution must be easy to deploy and use.
- It must offer deduplication, especially global client-side dedupe.
- It must provide flexible recovery options that offer high rates of backup frequency (multiple times per day for O365, and as often as every minute for endpoints), and it must offer the ability to set policies for RPOs.
- It must include SaaS data protection support, in particular for O365 data.
- It must come with advanced security including encryption, legal hold, data wipe, and geolocation tracking of lost devices—capabilities analogous to cell phone protection.
- It must be a proven technology from a proven vendor that offers comprehensive, always-available tech support.

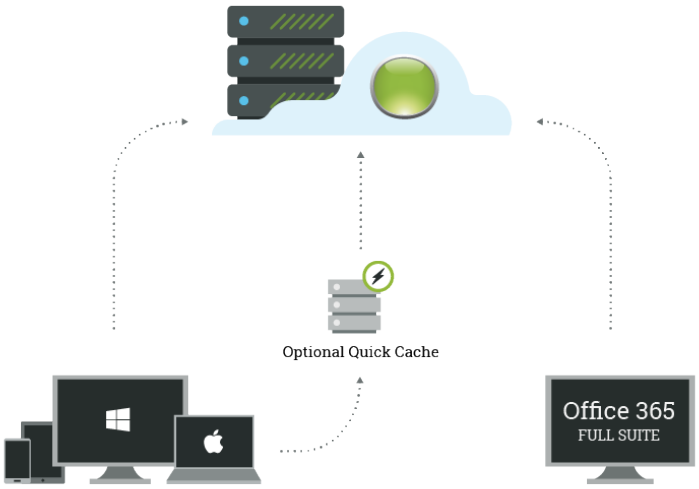
Carbonite Endpoint and Carbonite Backup for Office 365

Small and midsized organizations have particularly significant exposure, especially those with distributed or mobile workforces. They should be interested in Carbonite solutions, offering features necessary for robust and reliable protection and recovery of O365 and endpoint-stored data. Carbonite Endpoint and Carbonite Backup for Office 365 offers:

- Comprehensive, automatic backup for desktops, laptops, tablets, mobile devices, and the entire O365 suite including SharePoint, OneDrive, and Exchange. The centrally managed, policy-controlled backups can be set to occur as often as every minute for endpoints, and four times per day for O365 data.
- Protection against all forms of data loss, including lost or stolen devices, human error, and ransomware on both endpoint devices and within O365.
- Flexible recovery options including incremental restores of endpoint data, granular restores of O365 data, and point-in-time restores.
- Global client-side deduplication of AES 256-bit encrypted endpoint data.
- 256-bit AES encryption and mitigation features including global location tracking, remote data wipe, poison pill, and private key.
- Centralized, policy-based administration that won't interfere with end-users' productivity. Advanced administrative controls include legal hold, audit reporting, and role-based access.
- Remote data access from any device, anywhere, anytime.
- Geo-redundancy of data, plus global data center location options through Microsoft Azure.
- Device migration to move user profiles and settings between devices.
- Superior recovery support, available 24x7 from certified experts.

Figure 2 illustrates the solution architecture. The first step is to establish a centrally managed vault within Carbonite's Microsoft Azure-hosted vault. Next, the Carbonite software can be silently deployed on workers' computers, laptops, tablets, and smartphones using management tools such as SCCM, Intune, or LANDesk. The third step is to back up the devices using the local cache (or back them up directly to the central vault). At this point, the Carbonite solution is equipped to recover data as needed, or remotely wipe data if a device is lost or stolen.

Figure 2. Solution Architecture



Source: Carbonite

The Bigger Truth

IT must protect all data. However, protecting and recovering O365 data and data created by endpoint devices presents a distinct set of challenges. Data will keep on growing. BYOD environments will increase. The use of endpoint devices and software-as-a-service will only grow, too. And it is all happening in a context of heightened compliance and security risk.

Therefore, it is more imperative than ever to put data back under IT's control. Remember, it is all company data, and IT has to be responsible for all of it. IT needs to protect it from malware and ransomware. IT needs to be the organization finding the right ways to overcome the data sprawl associated with not eliminating redundant data before backing it up.

Those goals, and more, are achievable by properly incorporating activities such as dedupe, encryption, etc., into the protection process. Fortunately, Carbonite has excellent tools to help with the effort.