Research Brief

Endpoint Device Backup Trends

Date: April 2014 **Authors:** Jason Buffington, Senior Analyst; and Bill Lundell, Senior Research Analyst

Abstract: *There has never been so much corporate data outside of the data center as there is now. It is due to the changing usage of endpoint devices, particularly by users in bring-your-own-device (BYOD) environments. Too often, IT tries to utilize complex legacy data center backup approaches to protect these modern endpoints, with the result being that endpoints and all of the corporate data residing in them are left unprotected. But it doesn't have to be that way.*

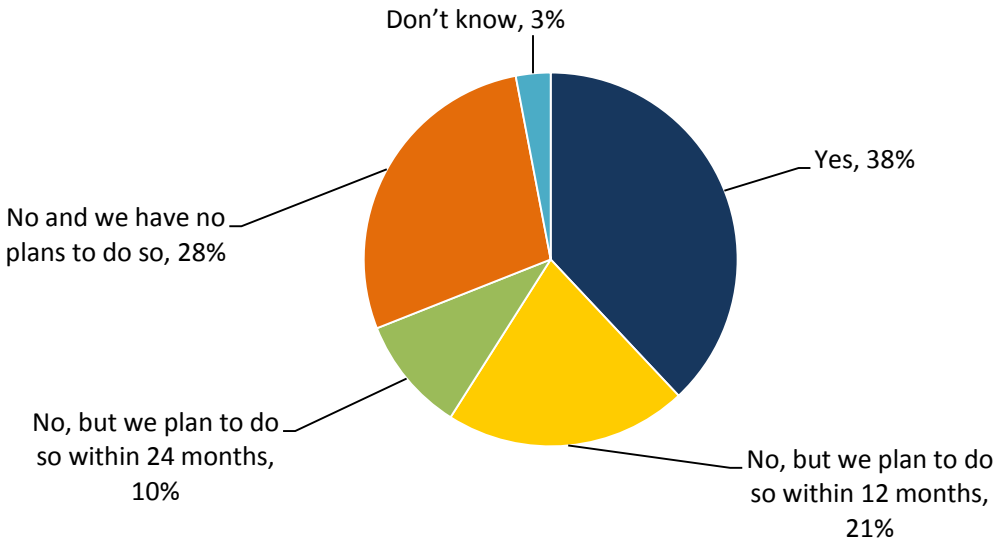
Backup Landscape for Endpoint Devices

ESG surveyed 306 IT professionals responsible for data protection technology decisions at small (20 to 99 employees), midmarket (100 to 999 employees), and enterprise-class (1,000 employees or more) organizations in North America.[1] While the focus of the research was the adoption and usage of cloud-based data protection services, respondents were also asked about the existence of an official policy to back up the endpoint devices (i.e., desktop/laptop PCs, smartphones, tablets, etc.) used by their organizations' employees.

As seen in Figure 1, more than one-third (38%) of respondents indicate that they have a formal process for protecting employees' endpoint devices. At the other end of the spectrum, 28% of organizations do not currently assign the responsibility of backing up endpoint devices to IT personnel, but rather delegate this task—and potential liability—to individual employees.

Figure 1. Formal Processes to Back Up Endpoint Devices

Does your organization have a formal process to back up the endpoint devices that employees use to do their jobs? (Percent of respondents, N=306)



Source: Enterprise Strategy Group, 2014.

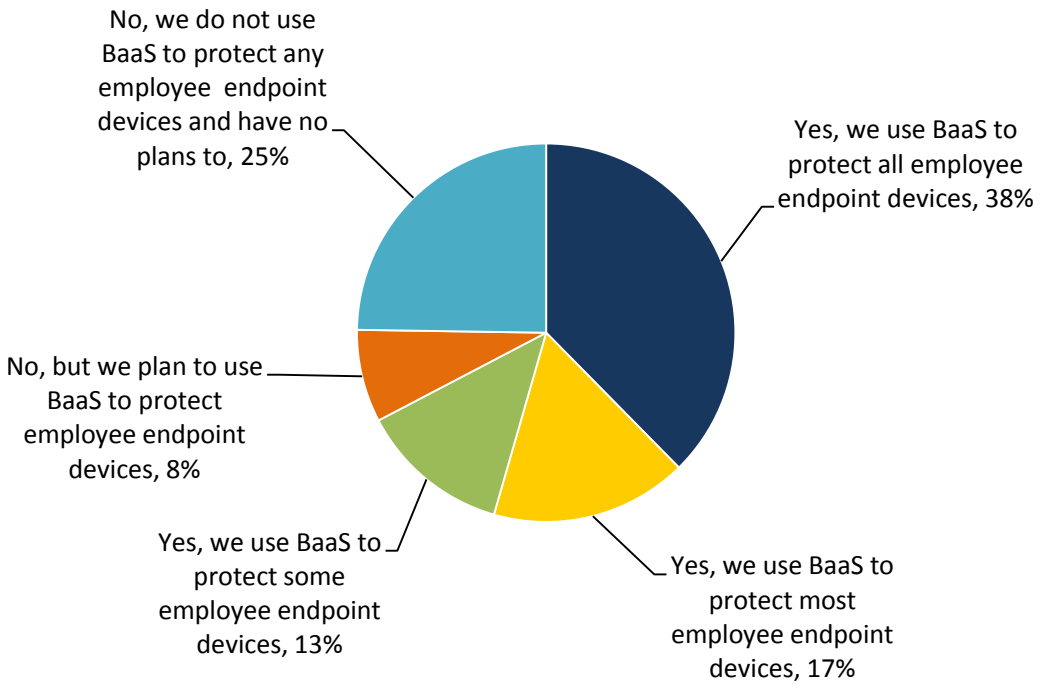
[1] Source: ESG Research Report, *Data Protection-as-a-service (DPaaS) Trends*, September 2013. All other ESG research references and figures in this research brief have been taken from this research report unless otherwise noted.

IT staffs are typically spread thin when it comes to managing and maintaining endpoint devices, an undertaking that is further complicated by bring-your-own-device (BYOD) policies. In fact, ESG research conducted earlier in 2013 revealed a ratio of several hundred endpoint devices for every administrator charged with supporting these devices.[2] With tasks like OS and application installations/upgrades and critical patching jobs consuming a lion's share of time, backing up endpoint devices is often viewed as a deferrable undertaking.

Because of these conflicting priorities and the prospect of trying to uplift legacy server-centric backup solutions to the 10x-50x additional endpoint devices (compared with servers), it is often hypothesized that the protection of endpoint devices is a strong candidate for cloud-based backup services and, according to Figure 2, more than two-thirds (68%) of *current BaaS users* already protect their employees' endpoint devices with these services, to varying degrees. In the context of those organizations with a formal policy to protect their employees' endpoint devices (as seen in Figure 1), approximately 14% currently use a cloud-based data backup service to some extent.

Figure 2. Protecting Endpoint Devices with Cloud-based Backup Services

Does your organization back up the endpoint devices that its employees use to do their jobs via BaaS? (Percent of respondents, N=24)



Source: Enterprise Strategy Group, 2014.

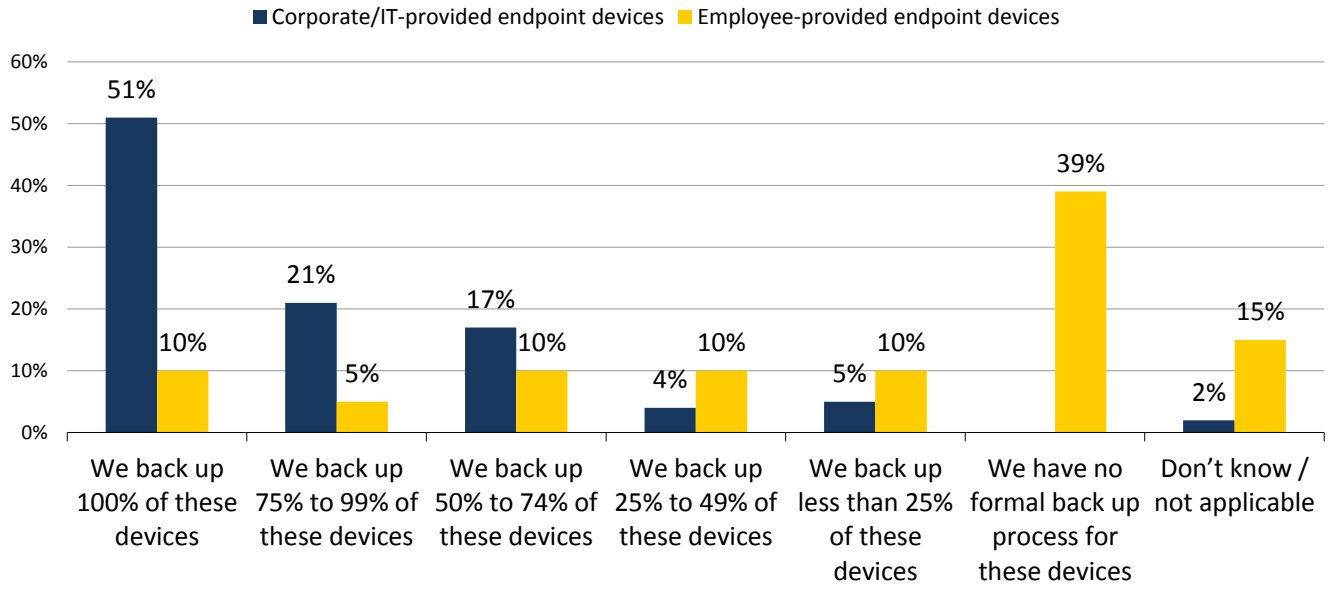
Among those organizations that formally back up endpoints, how pervasive are these policies in terms of the employees and devices protected? When it comes to the corporate-provided (i.e., paid for) endpoints supported by IT personnel, more than half (51%) report that every single device (i.e., 100%) is backed up, and 72% protect at least three-quarters of the PCs, smartphones, and tablets in their purview (see Figure 3).

The previously referenced BYOD trend further taxes already overburdened IT administrators, so it is not surprising to see employee-provided devices receive a reduced level of priority relative to those funded by the company. Specifically, more than half of organizations that formally back up endpoint devices either do not apply these policies to employee-provided devices (39%) or do not even know whether these devices are officially protected (15%).

[2] Source: ESG Research Report, *Desktop Virtualization Market Evolution*, February 2013.

Figure 3. Current Formal Backup Processes: Corporate-/IT-provided versus Employee-provided Devices

Please indicate the extent to which your IT organization currently has a formal process for backing up end-user endpoint devices, both those provided by the IT organization and those supplied by end-users themselves. (Percent of respondents, N=115)

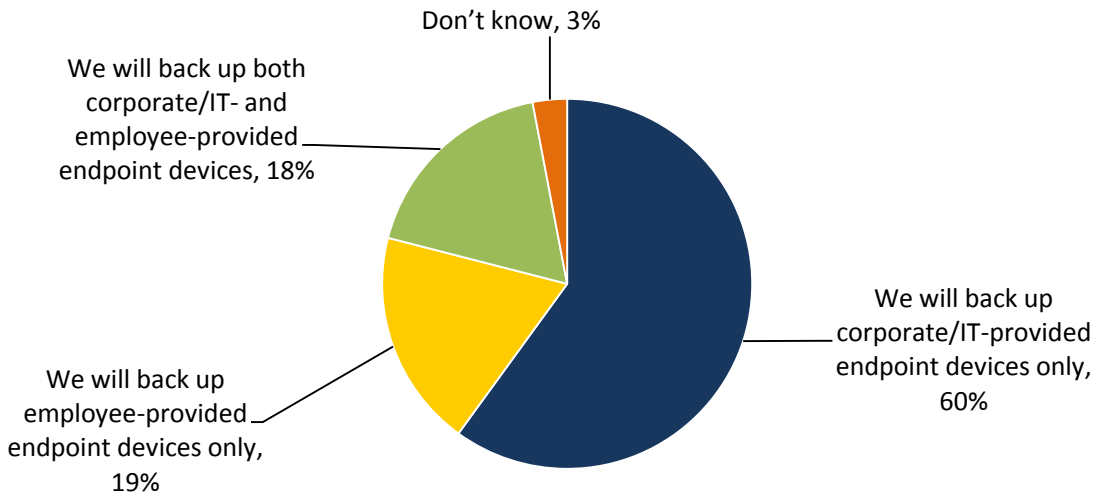


Source: Enterprise Strategy Group, 2014.

This trend looks to continue among yet-to-be-implemented formal backup policies, with 60% of those organizations with future protection plans for endpoints expecting to back up *only* corporate-/IT-provided devices (see Figure 4).

Figure 4. Expected Formal Backup Processes: Corporate-/IT-provided versus Employee-provided Devices

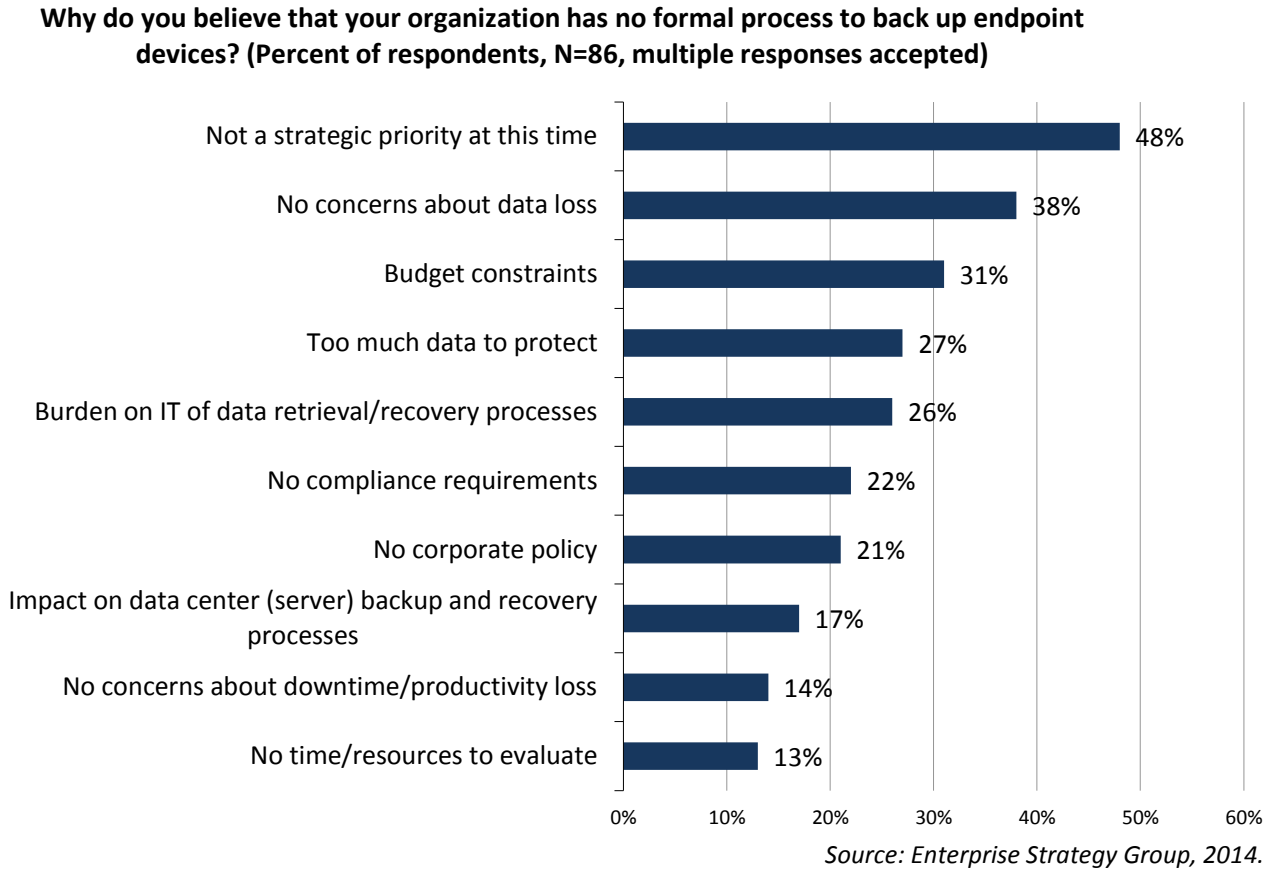
Please indicate which of the following endpoint devices you expect to back up? (Percent of respondents, N=95)



Source: Enterprise Strategy Group, 2014.

Nearly half (48%) of those organizations with no formal policy to back up endpoint devices take this position simply because they do not deem this process to be a strategic priority (see Figure 5). Anxiety related to data loss is clearly a key consideration for endpoint device data protection, so it is not surprising that 38% of those organizations with no plans to implement formal endpoint device backup processes lack those concerns.

Figure 5. Top Ten Reasons Why Organizations Have No Formal Processes to Back Up Endpoint Devices



Source: Enterprise Strategy Group, 2014.

The Bigger Truth

What some IT professionals have not internalized yet is that corporate data needs to be protected, regardless of where it resides. Most executives or business unit owners would be appalled if their IT staff decided that file servers were no longer going to be backed up, reserving protection for application platforms alone, because unstructured file growth was perceived as too hard and/or costly to back up. And yet, that is the attitude IT staffs are taking toward all of the miniature file servers' worth of data within endpoint devices. Others have taken a slightly less culpable stance of protecting corporate data on corporate endpoints (only), ignoring that any extra complexity of protecting BYOD or other non-IT-managed devices far outweighs the lost productivity of those users after a crisis or the lost effectiveness of an organization when a user leaves not only with his or her device, but also potentially with the only copy of data that ever existed.

Instead, IT has to recognize that corporate data has to be protected, regardless of whether it sits in a data center server, a cloud-based service, a corporate-issued laptop, or a device purchased by its user. Thankfully, cloud-based backup services and innovations from traditional backup vendors related to their endpoint protection capabilities can enable IT professionals to be *part of the solution, instead of part of the problem*.