ESG Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

A Better SaaS Protection Strategy for 2021: Protecting Knowledge Workers with Datto

Date: January 2021 **Authors:** Christophe Bertrand, Senior Analyst; and Monya Keane, Senior Research Analyst

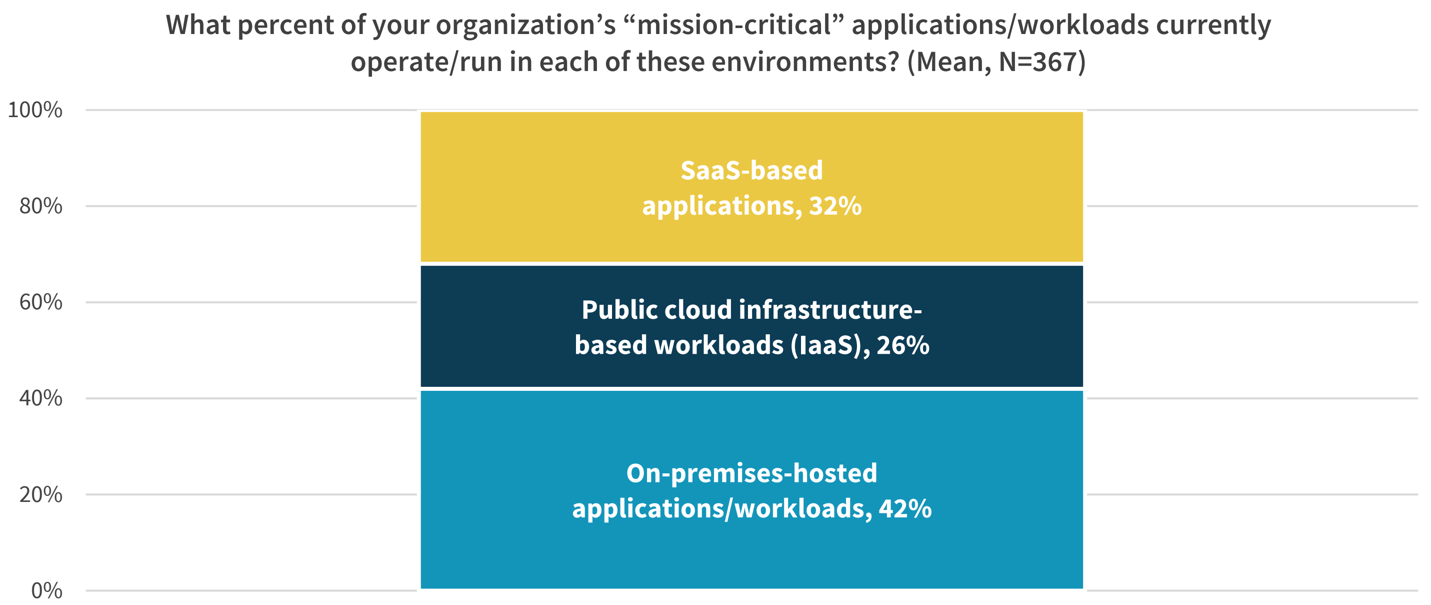
ABSTRACT: Both SMBs and MSPs have to maintain stringent SLAs for workloads such as Microsoft 365, just like big companies do. They need something that's easy to use, with automation and a full feature set. Just because they're midmarket, that doesn't mean they don't have stringent recovery point and recovery time objectives. Datto SaaS Protection is here—a cloud-to-cloud backup solution that offers comprehensive backup and recovery for mission-critical cloud data associated with Microsoft 365 and Google Workspace.

Market Landscape

New ESG survey research shows that 15% of organizations can tolerate no downtime at all for their mission-critical applications. Another 42% tell ESG that their mission-critical applications must be back online in one hour or less.[1]

In regard to where those mission-critical workloads reside (see Figure 1), it is very important to acknowledge just how much of a hybrid world we live in today. The majority of mission-critical workloads live offsite in the cloud now, rather than within a corporate data center. [2]

Figure 1. Where Do Mission-critical Applications Live?



Source: Enterprise Strategy Group

[1] Source: ESG Master Survey Results, *Real-world SLAs and Availability Requirements*, August 2020.
[2] ibid.

A similar evolution is affecting not just mission-critical data, but also the mission-critical employees who depend on it. Things certainly changed this year as millions of knowledge workers began working from home full time. ESG research shows that by late 2020, 56% of knowledge workers were operating out of their homes. And the vast majority of organizations appear to be content with their workforces staying away from the office for the foreseeable future. In addition, broader use of collaboration tools and increased adoption of cloud applications are the top-two most significant lasting business impacts on long-term IT strategy stemming from the recent health crisis.[3]

Those organizations are finding themselves faced with a need to update their recovery plans to accommodate new processes and protocols tied to current and future mass work-from-home mandates. For many companies, work-from-home may be here to stay. Cloud applications are already here—and growing—and that data is just as important to protect as on-prem data is.

SMB versus Enterprise Data Protection

Small and midsized businesses usually do not have as many in-house IT staff resources as big enterprises do, which is in part why they depend on managed service providers (MSPs) for help. Few "backup PhDs" exist inside SMBs.

But SMBs are just like large businesses when it comes to their need to protect mission-critical data and leverage it to conduct operations. Many times, data is the cornerstone of the entire business—or is at least a major element of business success. The crucial nature of data these days makes an SMB's ability (or inability) to always remain up and running more visible than ever. Data availability is now vital to instilling customer confidence and satisfaction.

And while their IT workflows might be simpler and smaller in scale than those within large enterprises, the same mechanisms still apply to data protection: SMBs still have to follow best practices to optimize RPO and RTO. Again, that is why they are relying on their service partners to provide that expertise and take over some or all protection-related responsibilities.

For these businesses, the assistance of a good MSP is now highly important against the backdrop of increasingly frequent cyberattacks and human error that causes data loss—all happening during our current work-from-home era.

SaaS Data Responsibility—a Shared Model

A big disconnect in the market exists when it comes to SaaS data protection. ESG research shows that 33% of surveyed IT decision makers report that they don't think SaaS data needs to be backed up. One in four report that they don't protect their Microsoft 365 data.[4] This is a potentially dangerous mistaken assumption.

It is important for organizations to know that their data is always theirs, not the service provider's, even though that data resides in the cloud service as part of a SaaS application. Recent outages at two major cloud providers also call into question how wise it really is to rely solely on the cloud service provider to protect mission-critical workloads.

From a backup and recovery standpoint specifically, it means organizations must put a third-party protection solution into place for all their platforms, both on premises and in the cloud. They may prefer to use an MSP to help deliver backup, recovery, and BC/DR as a function, but it is their ultimate responsibility. This is very important to remember. After all, data loss is a whole-business problem, not just an IT issue.

The consequences of downtime can be very negative to a business. It can have a direct impact on operational efficiency, employee morale, and customer confidence. And there are many ways to lose data, including some that are much more

[3] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey*, December 2020.
[4] Source: ESG Research Report, *The SaaS Data Protection Disconnect*, March 2020.

mundane occurrences than an external cyberattack. For example, 20% of ESG survey respondents report accidental deletion as the top cause of data loss related to their SaaS-based applications.[5] ESG research further shows that the estimated mean downtime of SaaS applications is one hour.[6]

Additionally, from a compliance standpoint, many organizations are required to demonstrate that they are protecting, retaining, and deleting data properly according to regulatory rules and privacy regulations.

It makes a lot of sense for an SMB to leverage a managed service provider to handle the often complex and skill-set-intensive activities associated with hardware, software, networking, power outage exposures, and physical protection. But regarding protection of data itself, the MSP will provide the primary support to help with recoveries associated with human error, programmatic errors, malicious activity, and practically any other data protection issue.

Datto Solution Overview

Datto SaaS Protection is a cloud-to-cloud backup solution that offers comprehensive backup and recovery for mission-critical cloud data associated with Microsoft 365 and Google Workspace. It is designed specifically for MSPs to protect their clients' SaaS data efficiently and manage client data retention, licenses, and cost.

Datto SaaS Protection protects against permanent data loss and allows MSPs to easily recover clients' data following a ransomware attack or other data-loss event with 3x daily point-in-time backups, managed through one pane of glass. The backups are stored securely in the Datto Cloud with files, folders, settings, and permissions intact for fast restores of everything from a single item to an entire user account. Datta SaaS Protection delivers backup, search, restore, and export for Microsoft 365 and supports Exchange, Tasks, OneDrive, SharePoint, and Teams. For Google Workspace, Datto supports Gmail, Google Drive, Calendar, Contacts, and Shared Drives.

The Bigger Truth

Datto was one of the first vendors to bring Microsoft Teams protection to the market. Datto's timing was smart: No one is moving away from remote work anytime soon. Datto also was smart in establishing a strong network of MSP relationships to ensure end-user clients receive the caliber of SaaS data protection they need in these challenging times.

Outages happen—even to the biggest cloud providers. People make mistakes and accidentally lose files. And hackers still abound. If you are all working from home and have moved to the cloud, too, *you need to protect your data*. Datto is a thought leader in cloud data protection, and its technology delivers all the goods for SaaS.

[5] Source: ESG Master Survey Results, *Data Protection Cloud Strategies*, June 2019.
[6] Source: ESG Master Survey Results, *Real-world SLAs and Availability Requirements,* August 2020

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188