Remote Work at Enterprise Scale:
Strategies for Microsoft 365 Migration and Management

When the pandemic hit, government IT departments scrambled to ensure state and local public employees had the tools they needed to work from home productively. While many organizations were already piloting cloud-based productivity and collaboration tools such as Microsoft Teams, others had to pivot quickly to free, short-term trial versions. Now that the dust is settling, IT leaders are looking more closely at their long-term plans for telework and cloud migration. For many, Microsoft 365 is at the center of their strategies.

The cloud-based Microsoft 365 offers a level of scalability, flexibility, integration and mobility that is difficult to achieve with on-prem solutions alone. Workers can access the tools they need regardless of where they are and what device they use. IT teams can centralize and streamline user provisioning across on-prem and cloud environments to expedite user access, simplify administration and strengthen security. Organizations can shift from a capital-intensive model of hardware and software investments, ongoing maintenance and rapid obsolescence to a model that offers predictable licensing costs and up-to-date services that scale rapidly to meet current and future needs.

While Microsoft 365 offers many benefits, migrating to any cloud-based suite that touches on so many core aspects of daily work is a multi-faceted process. It requires careful planning and management to ensure a seamless user experience, optimize workflows, maintain productivity, ensure security and control migration costs.

The following strategies help ensure successful migration and management of Microsoft 365:

- **Understand your data and processes.** Understanding source data is the most important — and most time-consuming — step of any migration effort. It involves cataloging, analyzing and prioritizing content; documenting its exact location and where it needs to be moved; identifying and strategizing desired goals for the target destination; and correcting and finetuning current processes before migration.

"I've been involved with a lot of migrations over my career," says Paul Clanton, a former CIO for two different counties and now a senior fellow at the Center for Digital Government. "The ones that turned out best didn't just take current processes and duplicate them, but rather they made you look at your processes and what you were doing. They took more time up front, but they saved a ton of time, money and heartache on the back end."

- **Migrate user accounts and identities first.** Identity is at the core of the Microsoft 365 platform, underpinning seamless access to Microsoft 365 workloads, collaboration and more. It is also one of the more straightforward functions to migrate. Once user accounts and identities are moved to Active Directory for Azure, the next step is typically to move all the shared, personal data that is tied to each identity (e.g., OneDrive, My Sites, Google drives, etc.). Once these two pieces are in place, organizations can begin to build out email and more complex workloads in a modular fashion.

- **Decide which business processes will benefit most from being in the cloud.** A hybrid cloud provides the best of both worlds. The key is knowing which processes belong in the cloud and which should remain on premises. Putting processes in the cloud allows remote workers to access the tools and information they need from anywhere and with any device. The cloud also provides more processing power and bandwidth for collaboration and intensive workloads.

While some agencies must keep content on prem to maintain full control over it, cloud solutions have evolved substantially to address compliance, privacy and sovereignty concerns. In addition, emerging tools enable greater control over data in the cloud; for example, administrators can now define the location of their data in terms of geographic regions or identities within a multitenancy.

Adopt identity-based security and access control. Allowing access to resources based on a user's authenticated identity and permissions helps ensure the right people have the appropriate access at the right time. In addition, it helps eliminate potential loopholes and complexity (such as contradictory or customized permission levels in SharePoint) that can accidentally lead to users' receiving permissions they shouldn't have. Identity-based data protection also simplifies access management, enabling agencies to more easily put new governance policies and other controls in place.

Implement a comprehensive data backup and recovery strategy. To preserve the business value of Microsoft 365 data, organizations need to protect not only individual documents, emails and chat records, but also the context and connections surrounding content. To meet data protection, compliance and disaster recovery requirements, organizations must back up Microsoft 365 regularly — and in-house — so the IT team can restore mission-critical data more quickly in the event of a disaster. A mature strategy also includes maintaining multiple copies of data on different media (such as tape and disk) and in geographically separate locations.

In many cases, third-party tools are available to help execute these strategies correctly, efficiently and cost-effectively. In Howard County, Md., for example, the IT team is responsible for ensuring public employees have access to the data and systems they need to serve the county's 300,000 residents. The small tech team must also ensure those systems can only be accessed by the right people. When native tools could not provide needed functionality for this and other tasks, the county turned to a third-party Microsoft platform management solution. The set of tools ensures accurate and efficient account provisioning, group policy administration, change auditing, disaster recovery and more. Besides improving data protection, service availability, resilience and compliance, the solution saves the IT team hours of painstaking work.

TOOLS FOR MAXIMUM RESULTS WITH MINIMUM DISRUPTION

The right tool sets can simplify and improve Microsoft 365 migration, management and governance:

Migration assessment, execution and validation tools. While Microsoft 365 includes native migration tools, third-party tools can add tremendous value by providing more granular visibility and control and by simplifying and automating migration tasks. For example, leading third-party assessment tools provide detailed, graphically displayed inventories of what data will move easily, what data will require remediation and what can't be migrated.

Licensing visibility and optimization tools. To control costs and plan for the future, organizations need tools that help them understand which Microsoft 365 licenses they have, how they're being used and whether each user has the right license for their role. For example, these tools can help determine whether the pool of unused licenses is larger than necessary and whether certain individuals or groups have more expensive licenses than they need.

Auditing and data governance tools. While cloud models eliminate many in-house IT tasks, organizations are still responsible for critical duties such as ensuring proper permissions and auditing user activity in their hybrid environment. To ensure best practices are applied, organizations should consider tools that help with life cycle management of user groups, user activity monitoring, and prompt detection of and response to suspicious behavior or anomalies.

Adoption and expansion of Microsoft 365 initiatives is gaining momentum as remote work becomes a mainstay and state and local government leaders get real-world experience of the productivity, flexibility, scalability and cost savings that Microsoft 365 brings. In general, a phased approach is most successful. It helps minimize disruption and allows organizations to focus their time, money and effort on the data and processes that have the highest priority and greatest impact.

This piece was written and produced by the Center for Digital Government Content Studio, with information and input from Quest Software

PHOTO PROVIDED BY SHUTTERSTOCK.COM

Produced by: CENTER FOR DIGITAL GOVERNMENT

The Center for Digital Government, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century. **www.centerdigitalgov.com.**

For: Quest

Quest helps migrate, manage, and secure Microsoft environments whether on prem, online or a hybrid of the two, including Active Directory, Exchange, OneDrive for Business, SharePoint and Teams. Quest delivers the most comprehensive set of Office 365 and hybrid management solutions, including solutions from recently acquired Quadrotech and Binary Tree. **www.quest.com.**