Microsoft IT Showcase

Microsoft increases productivity and protects assets with OneDrive for Business

For several years, Core Services Engineering (CSE, formerly Microsoft IT) has used OneDrive for Business as the secure cloud storage and synchronization solution for user files and SharePoint team sites at Microsoft. OneDrive for Business—in coordination with Office 365 and Windows 10 authentication and security safeguards—delivers a highly secure and encrypted environment that we can audit at any time. We constantly scan for data loss and unintended data sharing. Robust policies protect work files and manage the de-provisioning process. We're also expanding Office 365 to multiple geographic (multi-geo) regions and Azure datacenters within an existing tenant.

More and more Microsoft employees are choosing OneDrive for Business. People want and need an intuitive storage and synchronization user experience that just works and keeps them productive. And we have an enterprise focus on security, reliability, and strong performance. OneDrive for Business delivers.

OneDrive or OneDrive for Business

It's important to draw a distinction between OneDrive and OneDrive for Business. From a user perspective, the look and feel of OneDrive and OneDrive for Business are identical, but they are different in key ways.

OneDrive is a personal cloud storage service for people to securely store and share their files and access them from any device. OneDrive for Business also provides online storage and sharing, but it's designed with business in mind. For example, data is encrypted at rest—at both the file and disk level. Powerful integration and co-authoring features in OneDrive for Business help bring teams together to share and collaborate on work. Many document collaboration features—like content approval and document workflows—are available, as well as integrations with company social networks like Yammer.

Importantly, OneDrive for Business gives administrators powerful security, auditing, and reporting tools. Configurable settings for administrators include:

- Nuanced user permissions.
- External file sharing controls.
- Default file link types.
- Sync settings.
- Notification settings.
- Information Rights Management (IRM) application.

Simple storage and synchronization

OneDrive for Business and the new OneDrive for Business sync client give people access to files from anywhere. It's seamlessly integrated with Office 365 and installed with Windows. OneDrive for Business offers simple sharing and storage on desktop, browser, and mobile devices. With OneDrive for Business, people can restore previous versions of their files—essentially a self-service disaster recovery function.

The OneDrive for Business sync client automatically syncs cloud files to the desktop, so people can edit or view files offline. It's a simple way to share and collaborate both inside and outside of an organization. Specific files and folders can be synced to a local device. Real-time coauthoring in apps like Word powers seamless collaboration, and files can be accessed from OneDrive or SharePoint team sites on mobile devices.

OneDrive for Business is extremely robust. The real-time synchronization success rate for OneDrive for Business with the new sync client is 99.5 percent. A typical cloud file synchronization solution maintains a real-time sync rate of 93 percent.

How synchronization works

With OneDrive for Business, files sync between local drives and Office 365 cloud storage in two ways. The first time someone signs into the OneDrive sync client, Windows creates the local OneDrive folder structure, which appears in File Explorer. When they create and save a file to the folder structure or move an existing file into the folders, the file is synced to the cloud. Files, folders, and the folder structure are duplicated in a corresponding Office 365 file storage area.

Files can also be saved directly to the Office 365 files location. If the user has configured OneDrive, that file or folder will replicate from the cloud to the local drive. The user can easily share files from Office 365 cloud storage or email a link. People can access files from any corporate-compliant device with the One Drive client installed on it, such as a phone, tablet, or laptop, as shown in Figure 1.

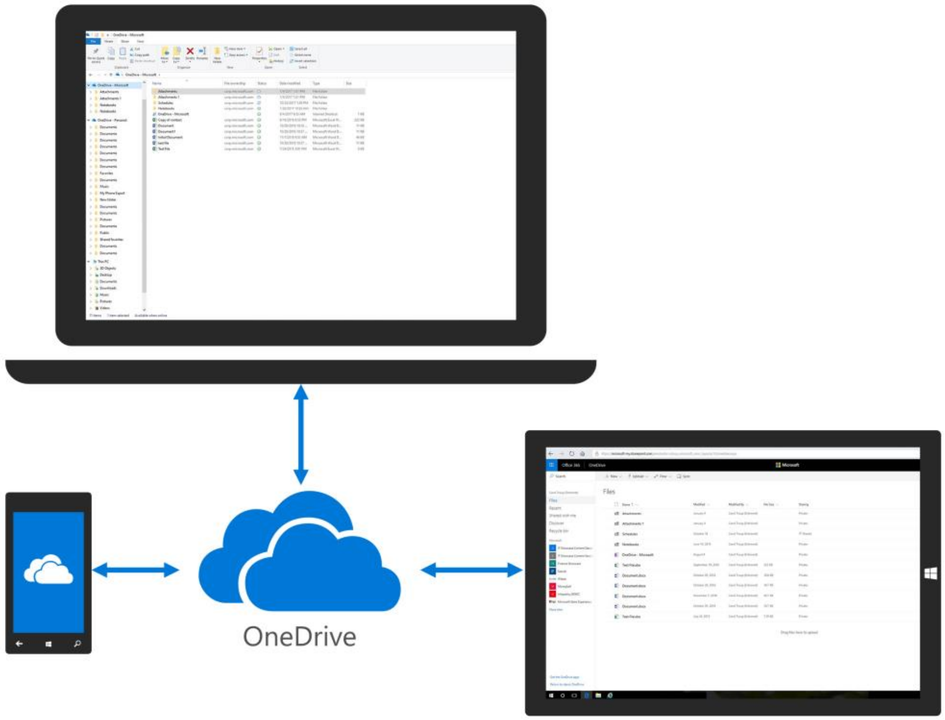


Figure 1. OneDrive syncs files between all employee devices

Direct cloud access with Files On-Demand

The OneDrive Files On-Demand feature was introduced with the Windows 10 Fall Creators Update. With Files On-Demand, people can access their files in the cloud without having to download them and use storage space on their device. All files—even online files—are visible in File Explorer and work seamlessly. Files On-Demand also allows users to open online files from the desktop or with Windows store apps using Windows File Picker. They simply select a file in File Picker and it automatically downloads and opens.

Powerful features spur migration

Major leaps in functionality and performance have allowed us to migrate most Microsoft employees to OneDrive for Business. It offers a clearly superior user experience and lets our people store vast numbers of files and SharePoint team site data. Each user has 5 TB of storage, with no maximum number of files or folders. Other advances include:

- **Special characters** are now largely supported in filenames. Outstanding unsupported special characters are an operating system limitation at this time.
- **Maximum file size** has increased to 15 GB from 2GB.
- **Maximum path length** has increased to 400 characters from 200 characters.

Users can now sync content from a SharePoint team site or an information rights management (IRM)-protected SharePoint site. As these features have come online, we've migrated people to the OneDrive for Business sync client and retired our old sync client, called Groove. Workers can safely and securely sync their corporate data from anywhere—which improves personal productivity and safeguards our corporate assets. Every computer imaged for a Microsoft employee now has the OneDrive for Business sync client pre-installed. It's also included in any Office 365 installation.

Strengthening security and compliance

OneDrive for Business keeps data secure and compliant. We have a largely hands-off and non-managed IT environment. Instead, we provide opt-in IT services, protect corporate assets, and we have strong audit policies.

Because OneDrive for Business inherits robust authentication methods from the Office 365 service, and it is a protected service—all files are encrypted by default and are audited when moved. CSE continues to invest in policy-based controls to offer a consistent user experience and to safeguard corporate data at the same time. New Windows 10 information protection features let us securely partition personal and business files.

Authenticate with Office 365

Because it is an Office 365 service, OneDrive for Business users authenticate with their usual Office 365 access method—either a domain-secured device or multifactor authentication with a password and phone authentication. Or, if the device complies with next-generation biometric credential systems like Windows Hello, it can bypass multifactor authentication completely. If a machine is not protected, the user has read-only access to files and folders through a browser.

We use private/public key authentication for both multifactor authentication and Windows Hello. Microsoft owns a single public key, and through Microsoft Active Directory (AD), federated services, and Azure Active Directory (Azure AD), we apply private keys to devices. The private key handshake must match our public key.

User accountability and strong policies

At Microsoft, we want to hold our users accountable for activities on their work devices and to protect corporate assets. We communicate often so that users understand risks and take responsibility for business files and company assets. The look and feel of the OneDrive for Business sync client is identical to the OneDrive sync client, which makes it easier for people to navigate between the two.

The ease of functionality between clients doesn’t mean that we compromise security. For example, we configure distinct OneDrive and OneDrive for Business folders, and we encrypt all data in OneDrive for Business folders. We don't restrict functionality in the app itself, but our IT administrators create policies and configuration standards to securely use OneDrive for Business in the corporate environment and enforce business rules. At a high level, here are some of the ways we do it:

- **Scan for sensitive data**. We use data loss prevention (DLP) policies to constantly scan OneDrive for Business files and folders for sensitive data.
- **Prevent unintended data sharing**. We use Windows Information Protection, introduced in the Windows 10 Anniversary Update, to differentiate between personal and business information. Windows Information Protection encrypts company data and helps to prevent inadvertent data sharing.
- **Default settings protect work.** We treat any file that is created on a work device as a work product. We’ve created a policy that changes one of the default settings for personal OneDrive accounts on our corporate computers. The policy changes OneDrive to default to a local directory and then synchronizes later to OneDrive for Business cloud storage.
- **Efficiently analyze events**. We configure Windows Event Forwarding to automatically transfer data audit events detected by Windows Information Protection to a storage location used by our Digital Security and Risk Engineering organization.
- **Safeguarded de-provisioning**. We’ve standardized and strengthened the way files are managed when an employee departs Microsoft, granting managers permission for a specific time period before files are deleted.

Data Loss Prevention

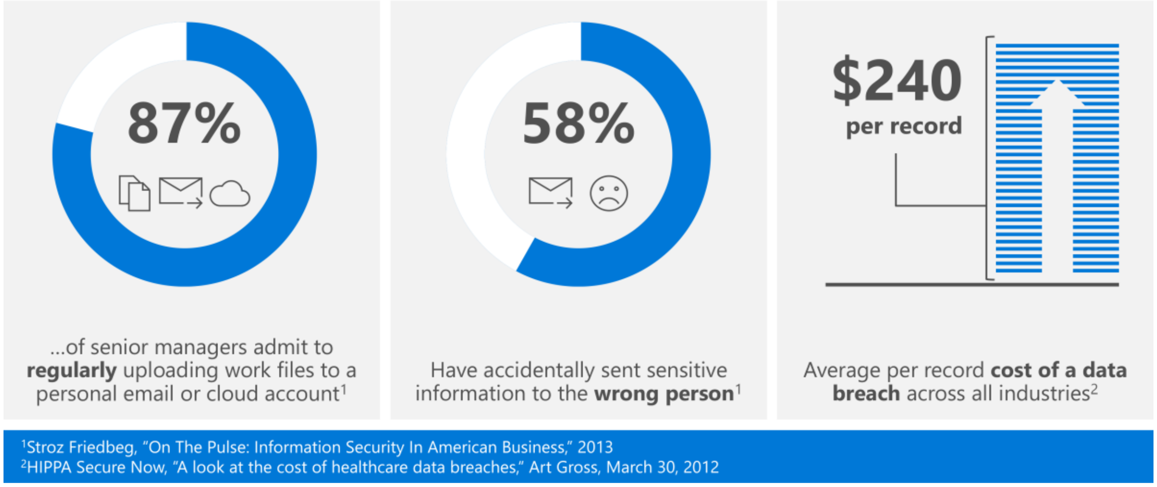
Internal tools protect sensitive information and prevent it from being inadvertently shared. Controls in the Office 365 Compliance Center allow us to easily set up DLP policies for OneDrive for Business.

At Microsoft, DLP policies constantly scan OneDrive for Business folders and tag and classify files identified as containing sensitive data that may not be properly protected. For example, they might contain personally identifiable information, like a social security number—or business data, like customer information. DLP then automatically notifies file owners, asks the file owner if the information is sensitive, and asks the file owner to follow up.

All OneDrive for Business files are encrypted, by default. Credential Vault Service applies an additional, unique layer of encryption, so that no other person—including a manager—can access someone’s OneDrive for Business files unless they are explicitly shared.

Windows Information Protection prevents data leaks

As the storage landscape gets more complicated, we're managing a constantly expanding web-enabled device environment. Data no longer automatically resides on-premises, and it's easier than ever for users to accidentally share information. Consider how simple it can be to copy or move sensitive business information to unauthorized, personal locations. Figure 2 shows the high cost of data leaks.



[1] Stroz Friedbeg, "On The Pulse: Information Security In American Business," 2013

[2] HIPPA Secure Now, "A look at the cost of healthcare data breaches," Art Gross, March 30, 2012

Figure 2. The cost of data leaks

Windows Information Protection—a new, file-level information protection service available in the Windows 10 Creators Update—supports the concurrent use and segregation of OneDrive for Business and OneDrive. It helps protect our corporate data and reduces inadvertent data loss incidents. Windows Information Protection, which is an out-of-box solution, used to be known as Enterprise Data Protection.

How it works

Windows Information Protection compiles a list of known corporate applications and resources, such as the corporate network or corporate cloud services. It uses those known data sources to identify business files, and assigns Microsoft as the file owner.

We operate Windows Information Protection in silent mode, which means that it doesn't interfere with our employee's work. That way if an employee moves files from a OneDrive for Business folder to a personal folder, the action is not blocked. However, the activity and corporate file ownership is logged in a database. That way, if something is compromised, we can audit the activity.

Windows Information Protection also scans for information that should be marked as confidential, such as personal information. It looks for files that have been moved or copied that have data that should be restricted, such as internal research, or protected SharePoint sites with files tagged as confidential.

Overall, Windows Information Protection metrics give us information on trends, such as common apps and usage scenarios, and gives us insight into what our users are doing with corporate data. Because audit logging data stays on the device, we use Windows Event Forwarding to transfer the events to a storage location used by our Digital Security and Risk Engineering organization. Windows Information Protection requires policy configurations in a mobile device management system, like Microsoft Intune, or in System Center Configuration Manager.

De-provisioning safeguards

When an employee leaves Microsoft, their AD or Azure AD account is immediately disabled. From then on, the Office 365 SharePoint Online User Profile Account (UPA) service launches. We use UPA, an out-of-box SharePoint Online service, that detects disabled accounts. UPA changes the user status to inactive, and nobody is allowed access.

UPA sends an automatic email to the departing employee's direct manager. The standard process is that the manager is granted permission for 30 days to check OneDrive for Business files and move or delete them as appropriate. After 30 days, the manager receives a final notification that the files will be deleted. Depending on the departing employee, Corporate, External, and Legal Affairs (the legal arm of Microsoft) retention policies may differ, and the retain or delete decision may be postponed.

GDPR compliance by default

The European Union (EU) General Data Compliance Regulation (GDCR) imposes complex rules on organizations that offer goods and services to people in the EU, or that collect and analyze data tied to EU residents—no matter where those businesses are. GDPR enhances personal privacy rights, and companies incur significant penalties for non-compliance.

OneDrive for Business programmatically complies with GDPR. Although CSE has access at a structural server level, there is no access to files or directories at the IT Pro level. We only use the DLP policies that are identified by our Digital Security and Risk Engineering team. DLP policies vary, depending on countries.

Managing an opt-in deployment

The cloud has turned everything upside down. Now, a deployment is less about pushing software out to users and is more about encouraging users to opt-in to a new service. For us, it meant increasing the number of users that sign into OneDrive for Business.

Our journey to a single storage and sync solution for Microsoft employees has been complex and not without some churn. For a long time, no single solution could meet all of our peoples' needs, and we had to support up to five storage and sync solutions at the same time. These other solutions included MySites, Work Folders, SharePoint team sites, IntelliMirror, and Windows File History.

Along the way, we've retired costly on-premises file servers, file shares, and SharePoint team sites like IntelliMirror and Work Folders. Decommissioning these systems has eliminated significant storage, infrastructure, and support costs.

Migration phases

As the OneDrive for Business sync client gained the capability to replace the old sync client, we completed a series of migration phases. Along the way, we've changed how we shut down legacy sync clients in increasingly nuanced ways and improved how the process works for our employees.

Until early 2016, Microsoft had 20,000 to 40,000 employees signed into an old sync client. We've made significant progress—and learned important lessons at the same time—through a series of sync client migrations. In the migration process, we get our users signed into the OneDrive for Business sync client, which takes over responsibilities from the old sync client.

Today, migration can be completely seamless for our users. For example, if people using the old sync client to synchronize a local SharePoint team site sign into the OneDrive for Business sync client, an app runs in the background to turn off the old sync client and turn on OneDrive for Business. Users are unaware that anything has changed—they just know that their site content is being synced.

MySites

We started with MySite site synchronization. MySites used to be the standard storage option at Microsoft. MySite users synchronized their corporate files or SharePoint team sites to cloud storage.

In this phase, the old sync client was deactivated and sync requests actually stopped working—it wasn't a great user experience. The OneDrive for Business sync client was already installed on computers, so people could have simply logged into it. Instead, users were guided to an installation link. The process served up confusing error messages and frustrated many people. This cost us—as many as 20 percent of our MySite users are still using the old sync client. We didn't communicate the experience well, and many costly support tickets were generated. We learned from this experience.

SharePoint team sites

Our next step was syncing SharePoint team sites. SharePoint team sites are used for collaborative sharing and co-authoring. Syncing these sites is extremely useful when employees are offline. They can work on content they are offline, like when they're on a plane, and then re-sync team site files when they land and get back online.

We had somewhere from 10,000 to 20,000 SharePoint team site owners synchronizing their site content. In this phase, we didn't want to disrupt our users by preventing the old sync client from working. However, if the user was already signed into the OneDrive for Business sync client on their computer, we would convert them over and synchronize seamlessly in the background. If the user wasn't signed in to the OneDrive for Business sync client, we would leave them on the old sync client and then notify them that the migration was coming.

So far, we’ve converted 80 percent of our SharePoint team site owners over, and it was a much smoother process than the MySites migration. The 20 percent of SharePoint team site owners that remain on the old sync client—those who weren’t already signed into the OneDrive for Business sync client—won’t be disrupted by a service interruption.

Information rights management-configured team sites

We also have some IRM-configured SharePoint team sites. These sites could not be immediately migrated from our old sync client to OneDrive for Business. Once we are able to, we will begin moving IRM-configured team sites to OneDrive for Business.

On-premises SharePoint sites

Finally, we need to migrate synchronization for our on-premises SharePoint sites. These are truly unmanaged shadow IT. Telemetry for our old sync client was not robust, and it’s hard to know how many on-premises SharePoint sites remain. We believe that there are less than 1,000. Migrating these sites might take many months—we’re trying to migrate all sites that we know of. At the same time, we’re trying to move as many on-premises SharePoint sites to SharePoint Online. SharePoint Online sites can be easily synced using the OneDrive for Business sync client.

We’ve addressed most product gaps, and we’re confident that the OneDrive for Business sync client can support most on-premises SharePoint site user scenarios. With few estimated users remaining, we’re planning to turn off the old synchronization service and remove it from our IT landscape. If a user has a valid need for the old service, we’ll find a way to return them to the old sync client.

We’ve eliminated Groove from all future Office updates and have removed it from our IT system images.

Communicating change

Digital transformation at Microsoft is happening at a breakneck pace. We’re taking a forward-thinking and systematic approach to managing change, and especially to communicating about it. A dedicated communications team in CSE helps ensure that each service update is communicated correctly, and OneDrive for Business is no exception.

You probably have some of the same challenges we do. While we can’t tell you how to implement your own change management program, we can—based on our own experience—provide some guidance on where you need to start communicating with your own users.

Framework for communication

We’ve built a framework that helps ensure consistent and high-quality communications campaigns. It’s built around three steps:

1. **Spark a campaign** with the right target audience, key message, and channels. Also establish your desired outcomes and known risks.
2. **Ignite engagement** by inspiring action from your audience. In this step, we build action plans and schedules, produce content and creative deliverables, manage campaign execution, and track goals with campaign reports.
3. **Add to the bonfire** by achieving sustainable business outcomes, driving cultural change, and establishing social norms that encourage quick action and draw people in to connect in new ways.

Without a strong communications framework, audiences can get confused—about what to do, when to do it, and why it matters. Support channels can get overwhelmed and flooded, and it can be hard for service teams to focus on a vision for growth. Employee productivity, a key factor in overall business health and growth, can decrease. And finally, without a structured communications framework, communications efforts will lack cohesion, as communications will probably be inconsistent and misaligned.

With OneDrive for Business, we’re helping our users with different content deliverables. First, in advance of change, we’ve created content that prepares and inspires them to use OneDrive for Business. Second, we communicate what people most need to know when change actually happens.

Prepare in advance

Our readiness deliverables include internal websites that share the value proposition of OneDrive for Business, guidance on getting started, and specific scenarios where OneDrive really shines, like real-time co-authoring, faster searches, and collaboration capabilities such as activity feeds and notifications.

When change happens

We're also communicating what people most need to know when change happens and updates roll out. Delivering the right information that people need precisely when they need it for each update is critical. In a cloud service environment, people on different release cadences receive different features at different times. First, we identify what information is relevant for people on each release cadence. Then our communications team identifies the best communication channels to use for each campaign.

Above all, we reserve direct emails for actionable communications—such as situations where our employees must do something to prevent a service interruption. We use less intrusive communication channels for informative messages, and emphasize how the changes can help employees do their jobs better.

The timing and cadences of communications matters. For example, we try to schedule email messages to be sent Monday through Thursday between 10 AM and 3 PM local time, with one message sent two days in advance, and another message the day of the change.

Exceptions

We are always trying to move on-premises, IT-managed files to our Azure infrastructure. While many of our individuals and teams now use OneDrive for Business, we do have some exceptions for extremely specific reasons that require on-premises file servers. These reasons include:

- Extremely high-availability data services.
- Extremely collaborative files.
- Legacy business intelligence systems.
- Partner sharing.
- Complex customizations.
- Extremely confidential files.

Multi-geo tenant architecture

Today, we have a large, centralized single-tenant Office 365 model. Performance is good overall, our tenant is huge, and we have established strong service between our Chicago disaster recovery site and our San Antonio datacenter, so we can failover to Chicago if necessary.

However, we’re moving toward a multi-geo tenant architecture model and eventually we want to expand to three locations, as shown in Figure 3.

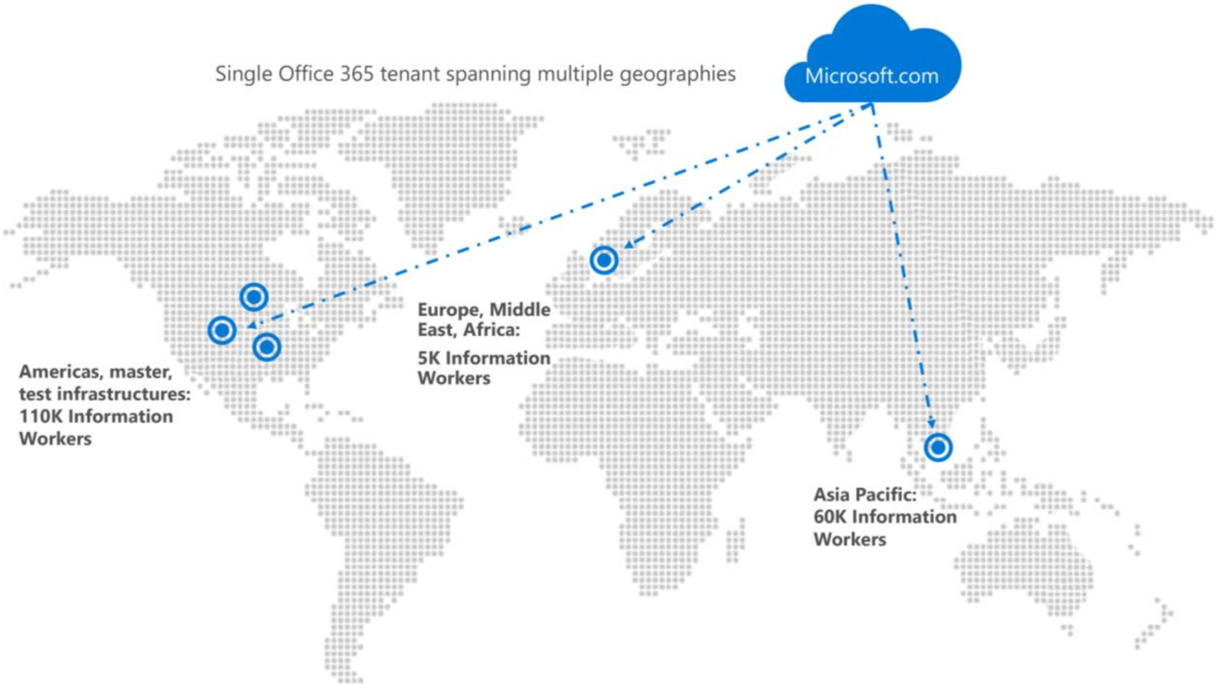

Single Office 365 tenant spanning multiple geographies
Microsoft.com
Americas, master, test infrastructures: 110K Information Workers
Europe, Middle East, Africa: 5K Information Workers
Asia Pacific: 60K Information Workers

Figure 3. Office 365 multi-geo infrastructure.

With multi-geo capabilities in OneDrive for Business, we can expand a single Office 365 presence to different regions and Azure datacenters within an existing tenant. Microsoft uses the North American site to manage the North American and South American regions, as well as housing what we call a master infrastructure. The master infrastructure is used to control, manage, and administer other locales. Additionally, the North American site houses a testing infrastructure that is internal to Microsoft.

Multi-geo lets us provision and store data at regional locations to meet data residency requirements. At the same time, we can globally roll out new productivity experiences to our workforce. Multi-geo is a good design for a large, global workforce, like Microsoft. It’s like a combination of PaaS and SaaS.

There are pros and cons to the multi-geo model. When tenants branch out, different licenses are required, as well as additional administrative engagements. However, employees might have better performance because they are closer to a network site. The downside is that some locations might be at capacity or have residency restrictions.

We are testing by moving a few teams to multi-geo, and it is complex. For example, every employee needs to have an Azure PreferredDataLocation (PDL) attribute set that must be reassigned in the shift to multi-geo. We’re handling it carefully as PDL affects lots of other apps in addition to OneDrive for Business—like Skype for Business, Microsoft Teams, Microsoft Exchange, and SharePoint Online. Once we get a PDL assigned to everyone, we'll start coordinating the moves.

Looking ahead

We want to take Windows Information Protection functionality much farther. Currently, we deploy Windows Information Protection in silent mode. It’s simply logging activity and not blocking anything. We’ll learn from experience, and then determine how to implement controls from there. We’re channeling feedback to the Windows Information Protection product development team. As blocking functionality becomes available, we’ll start to test it.

Some evolving functionality will help us migrate any remaining outliers. Autoaccount configuration will let us sign people in to the OneDrive for Business sync client by default when they sign in to their domain. This will help us nudge the old sync client users we couldn't convert by getting them automatically signed in and synced.

We want to expand what the OneDrive for Business folder structure stores and synchronizes to the cloud. Known folders—like Desktop, Documents, Pictures, Videos, and Downloads—could be re-mapped to the OneDrive for Business folder structure.

Also, we want to change the default Save location in Windows to the OneDrive for Business folder, whether it's local and synced or saved to the cloud.

Ultimately, the goal is to be able to replace a lost device or create a new device for employees, and to configure it to be identical to the old device, including files, apps, and app settings. If file and app data is stored in the cloud and linked to a profile, then configured apps download and run normally on a new device.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

From systems to people: rethinking service management

OneDrive sync client unifies client file storage and synchronization

Introducing Windows Information Protection

Windows Information Protection helps enforce data policy at Microsoft

Mobile, collaborative, and secure—Using Windows Information Protection to protect corporate data

Accelerate your path to GDPR compliance today