Twelve Smart Ways to Manage and Secure External Users in Your O365 Tenant

By Doug Barney

Microsoft Office 365 (now called Microsoft 365), is a superb productivity platform-- simplifying interactions between people, and empowering them to achieve more with colleagues and external actors. The huge benefit to bringing external users into your M365 tenant can be overshadowed by security risks, and provisioning and de-provisioning hassles.

This paper explores bringing external users onboard, ensuring their use of the tenant is safe, and how and why to remove them. Keep in mind, that in Microsoft 365 and Teams parlance, external users and guest users are the same.

1. Why External/Guest M365/O365 Users are Good

Microsoft 365 is amazing for employees to collaborate. However, partners, customers and other external users are also critical to the equation, and should participate in Microsoft 365-based work and communications. This involves:

- Being able to easily set up meetings and share calendars
- Share files in OneDrive or SharePoint
- Participate in Microsoft 365 groups.

An external/guest user is usually a non-employee, and refers to anyone that is not licensed or does not have an account registered in the organization's M365/O365 tenant.

There are two categories of external users – Authenticated and Anonymous.

Authenticated Users – People with a Microsoft 365 account based on a subscription to another account. These people can be assigned a license to your tenant and have the same level of permission as your employees or actual M365 license holders.

Anonymous Users – These users "can access a folder or document via a shareable link. Anonymous users can view, edit, or upload to the folder without having to log in with a username or password. Anonymous users cannot access sites, and you cannot assign licenses to them," Microsoft said.

Microsoft 365 is amazing for employees to collaborate. However, partners, customers and other external users are also critical to the equation, and should participate in Microsoft 365-based work and communications.

2. Risks Posed by External M365/O365 Users

The actions external users can perform is what makes them so dangerous. "An external user is authenticated when they have an identify account that can be Microsoft 365, or a different provider like Gmail. These people can work on your documents as well as be part of your M365/O365 groups. An anonymous user can access a folder or document through a shareable link, and view these documents without logging in with a user name and password," explained David Mascarella, CoreView Chief Global Strategist. "That makes this kind of collaboration very dangerous. External user accounts, for instance, cannot match your password security policy. And those credentials can be used to log in to multiple end user cloud services that are easier to hack."

External users are riskier than employees are since they are harder to secure, monitor, manage and control. Risks include:

- Anonymous external users making changes that admins cannot track
- Employees inadvertently sharing sensitive data with external users who were not the intended recipients
- External users accidently or purposely sharing sensitive information

"External users cannot be easily identified, and an anonymous link can be easily shared. External users can access SharePoint and OneDrive documents, as well as be part of multiple M365 groups, like distribution groups, Teams group, etc.," Mascarella added.

David Mascarella, CoreView Chief Global Strategist

"External users cannot be easily identified, and an anonymous link can be easily shared."

-David Mascarella

3. Minimizing Risks from External Users

Your M365 admin staff should insure the safety of external users by:

- Crafting a governance plan that determines what external users can do, data they can access, and what they can and cannot share
- Using Least Privilege Access to limit the rights of external users
- Disabling anonymous sharing
- Applying Data Loss Prevention (DLP) policies to automatically discover dangerous information sharing
- Disabling or limiting external sharing of sensitive data

4. External User Safety Checklist

There are nine main questions to answer to ensure external users interact safely with your M365/O365 tenant. Do you know?

- How many external users you have in your tenant, and how many are active versus inactive in the last 90 days?
- Who is taking care of provisioning and de-provisioning external users?
- What are external users doing in your tenant, including what files are being accessed, shared, and downloaded?
- How to access external user activity logs?
- What to do if an external account is breached?
- How to automatically notify external users that all activities are tracked, a log of accesses is kept for several years, and that they are responsible for keeping confidential information protected?
- Are you monitoring external account activities?
- Are you aware of files accessed by external users? Downloaded? Synchronized on their computers?
- Do you have a log of all activities performed by each external user?

If you answered no to more than one of these questions -- you really need CoreView to tighten external user controls.

5. Dealing with Stale External Users

Digital interactions between different companies is the core of productivity. M365-equipped employees share files with external users, invite them to share in Microsoft Teams chat or meetings, and add them to distribution groups every day.

Usually these interactions are limited in time, and the external user accesses a resource for a specific project or moment in time and then goes back to his normal activity. Unfortunately, this guest account is still active in the tenant and he can login whenever he wants.

What happens if his account is breached several months after invitation? The attacker will be able to access shared resources, read emails exchanged, and act on behalf of the real users. What happens if the employee who invited him leaves the company? Who is responsible for removing the guest user from the tenant? Probably it will remain there forever.

CoreView addresses all these problems through a workflow that can be used to force users to add detailed information when an external user is invited such as department, company, manager, country and a validity. CoreView will take care of removing the invited user or renew it based on a customizable approval process.

CoreView automation can also be used to identify external users inactive in the last 60 days and automatically start a process of cleanup with approval. Any external user is an additional endpoint to your tenant -- keeping them active indefinitely is a common bad practice that can be easily addressed with CoreView.

CoreFlow will take care of removing the invited user or renew it based on a customizable approval process.

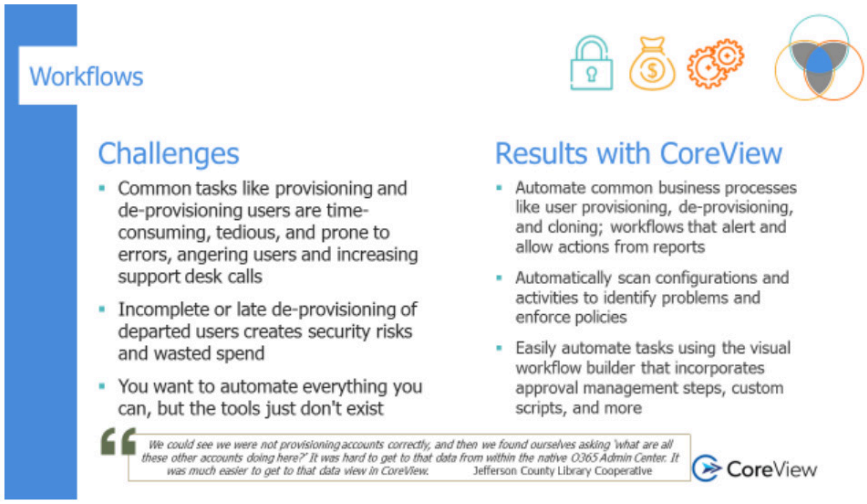
CoreView automation can also be used to identify external users inactive in the last 60 days and automatically start a process of cleanup with approval.

6. How Workflows Automate External User Management

CoreView addresses myriad external users and their issues through workflows, which are handled by CoreView's CoreFlow. A prime example is a workflow that forces employees to add detailed information when an external user is invited such as department, company, manager, country and a validity. CoreFlow will take care of removing the invited user or renew it based on a customizable approval process. CoreView automation can also be used to identify external users inactive in the last 60 days and automatically start a process of cleanup with approval.

Any external user is an additional endpoint to your tenant -- keeping them active indefinitely is a common bad practice that can be easily addressed with CoreFlow.

Adding CoreFlow automation to the external user equation makes it faster, easier and safer to perform external user processes. Chief Technology Officer Ivan Fioravanti detailed how CoreView does this work. "Maybe you do not want the M365 operator to go manually through all the external users. A second way is to run a workflow. Built into the platform we have CoreFlow, which does business process automation," Fioravanti said.



Here the M365 admin can select external users from within the CoreView management interface, and click 'Execute Workflow'. The admin can launch a predefined workflow, say "Remove External User'. This workflow automatically picks up all the information from the table of external users, including 'User Name', Last M365 Activity', name of 'Manager', 'Display Name', and 'Primary SMTP Address'. "From this workflow, an operator approval will be sent to remove user, and email sent to the manager asking if this external user can be removed or not. If the manager clicks consent, the external user will be removed and email will be sent to the external user. Otherwise, the external user will remain in the tenant," Fioravanti said, adding that crafting these workflows is so easy that "building the workflow is like playing with Legos."

Workflow scheduling is flexible and easy. "Maybe we want a Monday morning habit of dealing with external users. You can schedule the 'Inactive External User' report, and have IT alerted if it is not empty. So you choose every week. The action is that the workflow will automatically execute, and send an email to the manager asking to remove the external user. You can always re-invite an external user that has been removed," Fioravanti said.

Adding CoreFlow automation to the external user equation makes it faster, easier and safer to perform external user processes. Chief Technology Officer Ivan Fioravanti detailed how CoreView does this work. "Maybe you do not want the M365 operator to go manually through all the external users. A second way is to run a workflow. Built into the platform we have CoreFlow, which does business process automation," Fioravanti said.

CoreFlow adds to external user security. "Everything is extremely secure. You can create a workflow that will only be visible to specific users, specific operators of the platform. Using RBAC and virtual tenants, only that operator can see and use that workflow," Fioravanti said.

7. Monitor and Control External Sign-ins to Azure AD

Allowing external users access to the M365 tenant, or using the external sharing features of SharePoint Online or OneDrive to share content with people outside your organization, raises the bar for monitoring Azure AD sign-ins to look for unapproved users, or improper actions by external users.

M365/O365 admins must closely monitor those external access privileges and keep track of the associated activities. A standard requirement for Microsoft 365 administrators is creating a list of all resources that were accessed by users outside of the organization.

That is why CoreView created a "Sign-ins External" report. With this report, Microsoft 365 admins easily visualize who performed the external access, when it happened, what content the external user has access to and from what geographic location. CoreView enhanced this report with geo representation for location mapping searches, along with pivot point analysis from directly inside the report.

Allowing external users access to the M365 tenant, or using the external sharing features of SharePoint Online or OneDrive to share content with people outside your organization, raises the bar for monitoring Azure AD sign-ins to look for unapproved users, or improper actions by external users.

8. Provisioning and De-Provisioning External Users

There are two approaches to external/guest user provisioning -- manual and automated. With the manual approach, which with CoreView is not entirely manual, CoreView has a management wizard to invite the guest user, create a screen name, display name, email address, and create a personal message with the invitation. Guest users' details include title, department, phone numbers, street address, usage location, and the manager that invited the guest. "Including the manager is extremely important because this can be used to achieve not only the visibility, but used to notify the user who invited the external user when we want to delete it," Fioravanti said.

Onboarding an external user is easy, and ensures safety when done through CoreView. "You send an email to an external user with your policy, or have CoreView identity that an external user has been invited, which we track from

the audit log. CoreView then sends the external user an email with your policy, and you can have a workflow that sends that user all the needed information on best practices and company rules to access information," Mascarella explained.

9. How CoreView Manages and Secures O365 External Users

Your M365 admin staff can use CoreView to ensure the safety of the external user. "Managing external users is very important. Digital interaction between many companies is the core of productivity. M365 lets you share files with external users, invite them to share in Teams chat, join a meeting, or have them in groups every day," Mascarella said. "Usually those interactions are limited in time, and the external user access is for a specific project or moment in time, then they go back to their normal activity. Unfortunately, this guest account is still active in the tenant, and they can log in whenever they want. What happens if this account is breached several months after limitation? The attacker will be able to access the shared resources, read the emails exchanged, and act on behalf of the real user. What happens if an employee who invited himself with his own Gmail credential leaves the company, who is responsible for removing guest users from the tenant? Probably it will remain there forever."

What happens if this account is breached several months after limitation?

The attacker will be able to access the shared resources, read the emails exchanged, and act on behalf of the real user.

CoreView Chief Technology Officer Ivan Fioravanti explained in detail how to manage external users.

Ivan Fioravanti, CoreView Chief Technology Officer

With CoreView, an admin can first analyze the external user in the tenant. "First, how many external users do you have? CoreView has 200 reports, so you can click guest user to see a list of users in the selected tenant, and the number. If you want more info on an external user, you can look at department and manager that invited the external user," Fioravanti explained.

10. Track External User Activity

Tracking guest users is critical for safety. "How can we track the inactive external user? Usually the interaction with an external user is simple. There is someone we want to work with. We invite him to Teams, and maybe want to share a document. After that, quite often the interaction is finished. 90% of the interaction is finished when we share something," Fioravanti said. "IT can use the compliance dashboard. In the security of external users section, IT can also create a report for tracking 'Inactive Guest User in the Last 30 Days'. This gives the full list of inactive users in the last 30 days."

From this report, an admin can take different actions. "First, we can manually remove one of them because they are no longer needed. And every time we take an action here, we can take notes – why we are performing this action. This is very important for visibility," Fioravanti said.

IT can also see what the external user is doing in the tenant. This starts with the audit tab, where CoreView collects any activity on the tenant, for example if an external user was invited to share a file on SharePoint, or OneDrive, or if that external user was added to Teams. "I can go to OneDrive, check for external invitations, and go back the last six months (CoreView has unlimited retention of data). If something happened, you can drill down and see exactly what happened with that external user. The system shows a list of all external users invited to OneDrive, you have the detail needed to see what is going on," Fioravanti said. "I can look at SharePoint, drill down into external access, and see all external activity over a period of time. I can see the details, such as source file extension, creation time, site URL, operation performed, modified files, accessed files, and downloaded files. For downloaded files, we can get a list of all files downloaded by an external user."

Knowing when files are deleted is important. With CoreView, IT can look at deleted files (by external user), and create alerts notifying admins of external user actions such as file deletion. This can be tracked in a granular way, such as action, department, etc. "This can become an alert or a workflow, where IT can be notified or immediately take action. You can send an email to the external user stating 'you have deleted this file, are you sure it was intended?'" Fioravanti said.

Knowing when files are deleted is important. With CoreView, IT can look at deleted files (by external user), and create alerts notifying admins of external user actions such as file deletion.

11. Find Where External Users Are

External users can be everywhere across the tenant. The good news is CoreView can find them. For instance, IT can go to the Office Group, see all external users, and what groups they are part of. The same can be done on the Teams side, because behind Teams there is an O365 group. Here IT can go to the Teams report, see Teams members, and even a list of external users and the Teams groups they can access.

It is important to discover what is going on. Fortunately, discovery is quite easy. You simply create a dashboard tracking 'Security – External Users'. The dashboard can show:

- External users in Distribution Groups
- Files or folders deleted by external users
- Total external users
- External users in O365 groups
- New external user in last 7 days
- Inactive quest users in last 30 days

IT is alerted to issues and can drill down for more detail.

12. The Pain: Sensitive Files are Shared Externally.

With native Microsoft 365 security, intercepting the sharing of sensitive and confidential files is nearly impossible. IT can create alerts on a per file basis or per user basis and notify IT or a group of users – but this approach is ineffective. IT receives thousands of alerts per day: these new alerts are just extra noise in an already loud world.

In a CoreView world, when a user from the sales department, for instance, (CoreView's unique enriched audit log grants the capability to identity users by location or department) shares a file with an external user, a workflow starts. This notifies the user sharing the file, his/her manager, and the external user that this activity has been logged, and any following activities on the file will be audited. In this case, IT is not even involved, responsibility is shared among all actors involved and security is increased.

In a CoreView world, when a user from the sales department, for instance, (CoreView's unique enriched audit log grants the capability to identity users by location or department) shares a file with an external user, a workflow starts.

OneDrive being shared with external users is a particular pain point and security threat, and is something CoreView easily addresses.

External users should be informed of what they can and cannot do. "Clearly, this is not offered by O365. O365 is the infrastructure, but in the end, everything is based on the people using it. Admins have the responsibly of picking up the data, because Microsoft is not doing pickup. Admin also defines the policy, who can do what are up to the admin staff," Fioravanti said. "Disabling anonymous links, for example. I strongly suggest you do that, but by default, it is there in O365. What the external user can and cannot do – admins have to define it. Admins have to tend to your employees, and define how they can share in a secure way. The best way is the first time you invite an external user, send them terms and conditions or basic rules, to access company files. This can be automated via a workflow, for the external user provisioning."

CoreView's Mascarella agrees. "Sometimes an external user has to access sensitive information. You want to inform them and get an acknowledgement that they use that information only for that job. They cannot share that info. You should collect that acknowledgement," Mascarella said.

Become a M365 External User Security Expert

Learn more at our Webinar How Do You Manage External Users in Your Tenant?.

Learn more about making remote workers happy and productive with a CoreView demo.

Get your O365 user workload usage and security profile FREE with our new CoreDiscovery solution. You can get your free software now at the CoreDiscovery sign up page: https://www.coreview.com/core-discovery-sign-up/

Doug Barney was the founding editor of Redmond Magazine, Redmond Channel Partner, Redmond Developer News and Virtualization Review. Doug also served as Executive Editor of Network World, Editor in Chief of AmigaWorld, and Editor in Chief of Network Computing.