Aligning your digital collaboration **to zero trust**

How a least-privileged approach to users, data and workspaces can secure collaboration without impeding the mission

Jay Leask

AvePoint

Traditional zero trust models on which cybersecurity focuses on are typically at the network, applications or services endpoints, and a user's login. However, as more federal agencies and the defense industrial base (DIB) continue migration toward cloud solutions like Microsoft 365, cybersecurity must realize that system-level security policies will struggle to protect and enforce in collaborative environments.

Cybersecurity and IT will need to come together and examine the different paths through which a user could access sensitive information, how workspaces are provisioned and monitored, and what roles guest users play in the environment.

Protect information by setting policies at the workspace level

Federal agencies and the DIB work with the most critical information, ranging from scientific research and health care to civilian information and classified defense assets. It has always been their responsibility to safeguard this information from those with malicious intent.

For the above reason, it is essential to ask questions about the expected use and desired security for a workspace based on the data type that will exist there. For example, if a Defense Department agency requires all information tagged as highly sensitive and classified, IT administrators could create a questionnaire to guide an end user to create a new workspace that will enforce the right policies based on the information that will live in it.

A DIB organization could apply the same workspace policy enforcement. For example, the organization could have a policy about what types of sensitive information would be available in specific Microsoft Teams to block the ability for anyone who is not U.S.-based to access the sensitive information. By focusing on the workspace level instead of the file level, we can identify high-risk areas and, on the flip side, make it easier to collaborate on non-sensitive information.

Tailor permissions for external users

Guest access provides people outside your organization access to content inside your M365 workspaces (i.e., Teams, SharePoint and Groups). A health care-focused agency could use guest accounts to collaborate with grantees and their site staff or academic researchers. A defense-focused agency could use guest access to coordinate with local law enforcement to plan incident response or correspond about special event planning.

Despite the benefits, agencies need policies and reporting when using features like guest access to ensure your information stays protected. There are three things your agency can do today to ensure guests only have access where absolutely necessary:

1. Consider conditional, multi-stage processes when

Nick Iliasov

> It is essential to ask questions about the expected use and desired security for a workspace **based on the data type that will exist there.”**

onboarding a new guest into your workspace. Guiding users through a questionnaire as they set up the workspace will help determine if guest access is appropriate.

2. Create a guest monitoring program once they have access. Gaining visibility should allow you to track any suspicious activity and identify potentially sensitive information exposure tenant-wide.

3. Scale policy enforcement through automated rules for access, settings or other configurations based on your M365 Groups.

It might feel counterintuitive to allow sensitive information into a collaborative solution while staying within the zero trust principles. After all, there is no better way to secure your network and application than by restricting access to only a select few. However, it’s important to remember that collaboration has always happened — through sanctioned (email, extranets, etc.) or unsanctioned (shadow IT) methods. With some of the tactics above, an agency should be able to create the digital collaborative space it needs to complete its mission while securing it from potential threats. ■

Jay Leask is director of federal strategy for AvePoint Public Sector.