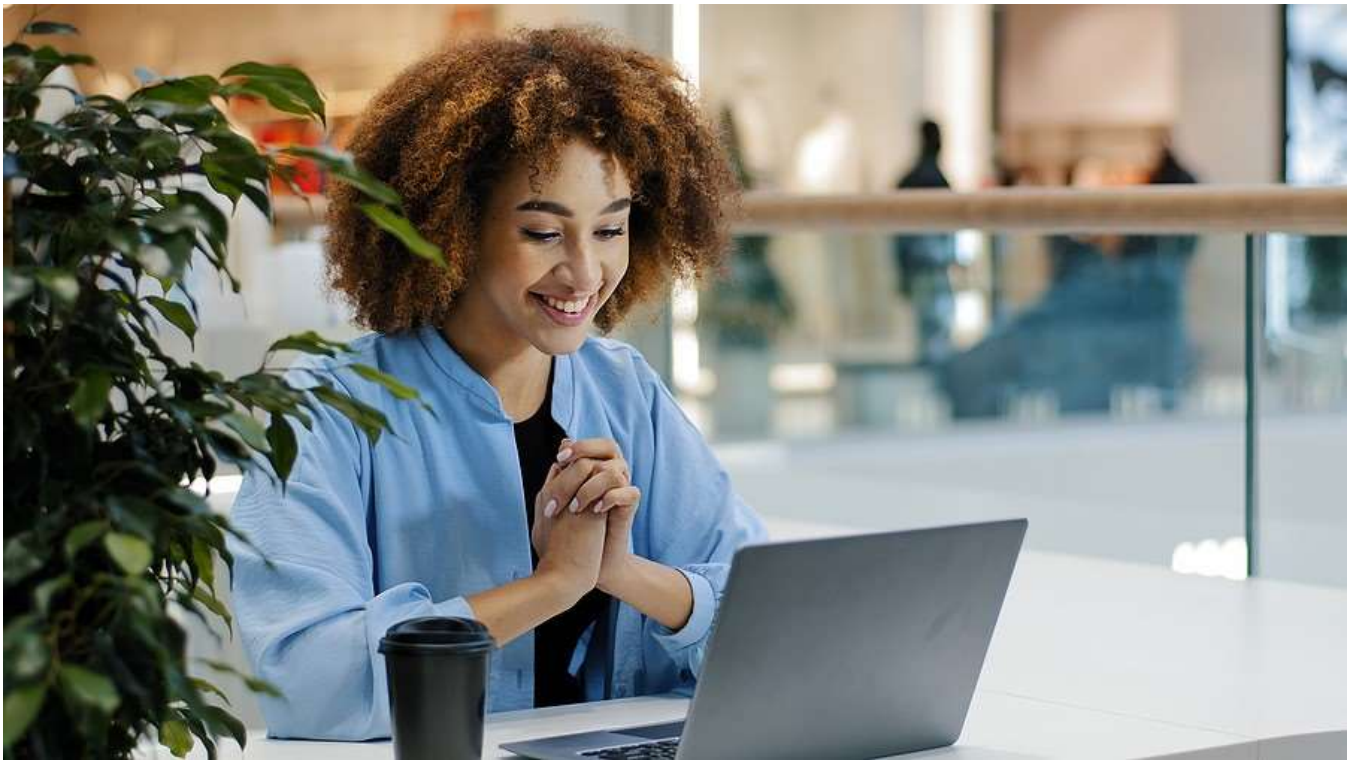
Protect Your Business from Risky App Usage with Microsoft Defender for Cloud Apps



Modern workers have thousands of apps at their disposal to help them collaborate and to streamline their work. However, when they use apps not sanctioned and controlled by the organization, they introduce risk. Wise administrators take a balanced approach to risky app usage by combining technology with user education and open communication.

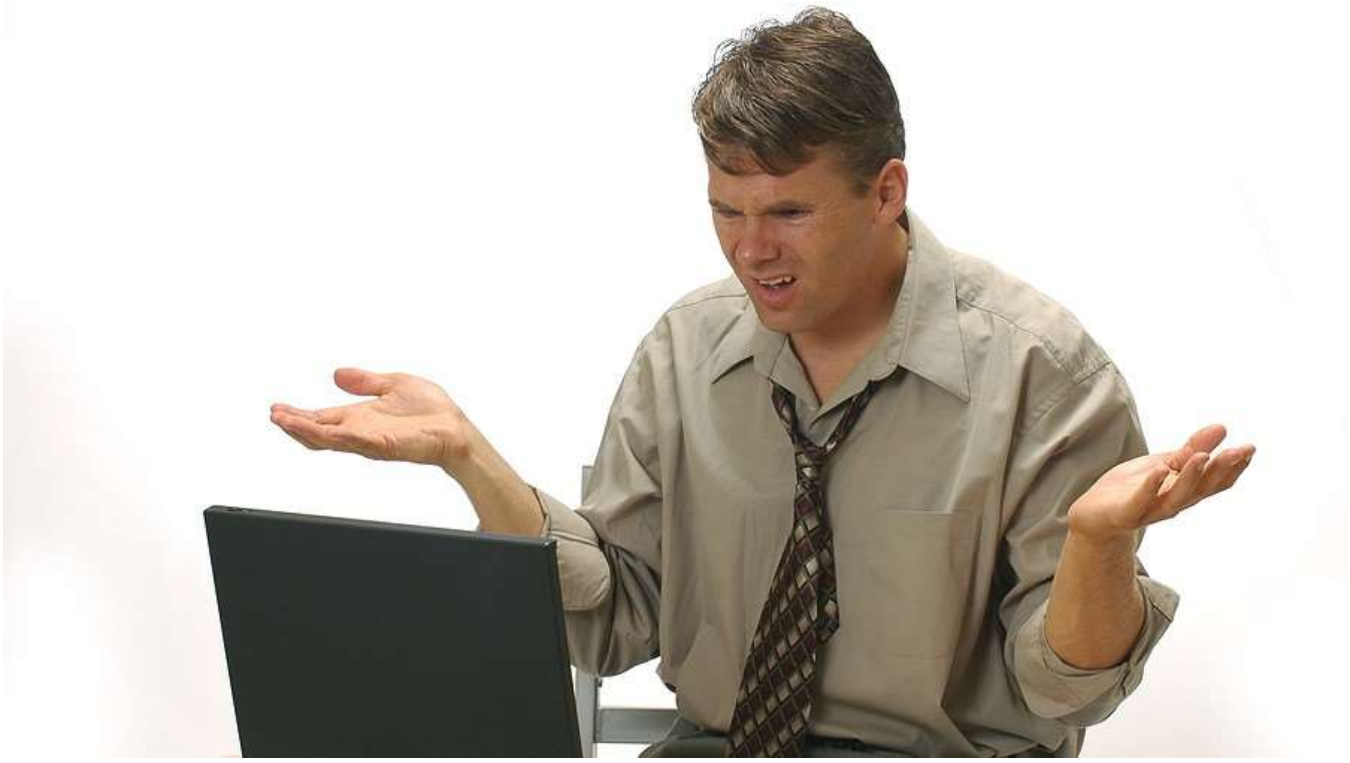
Shadow IT refers to the apps, devices, and other technology that employees use without the knowledge of the IT department. Often, employees use unsanctioned apps to increase their efficiency or because the approved apps feel too complex or lack desired features. Unfortunately, the employees may not recognize the security risks posted by shadow IT.

Common Types of Shadow IT

Remote work has increased the use of shadow IT as users try to work around several typical challenges. For instance, one common area of risky app usage involves file storage. Employees working from home may find it easier to store work files using the apps they use for personal files.

Tools for collaboration and productivity represent another risky area, especially when collaborating with colleagues outside the company network. The fastest way to share a file or conduct a remote meeting might involve cloud services outside the approved list.

A third common source of risky app usage involves communication. Messaging apps may seem harmless, but when employees share business-related information via unsecured messaging tools, they create vulnerabilities. Likewise, mixing work and personal email can result in unintentional data leaks.



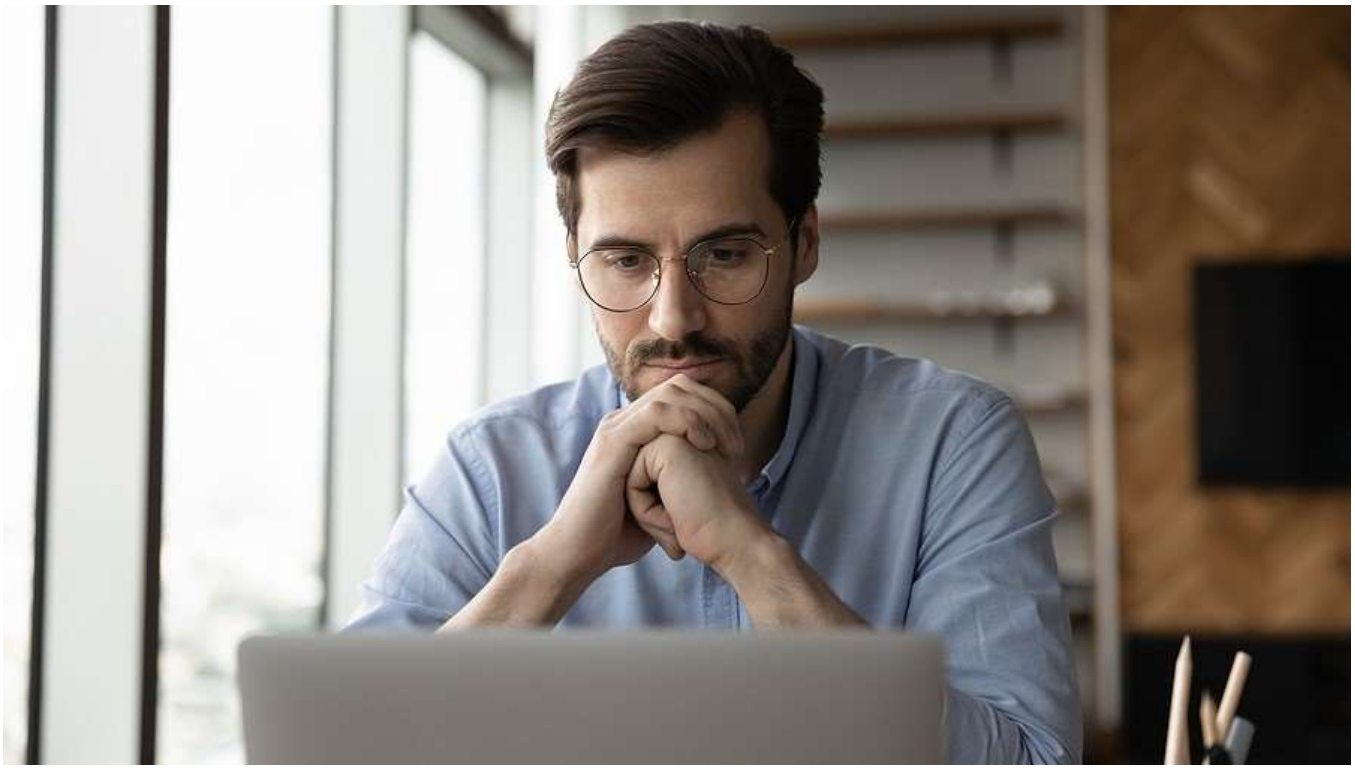
Risks Posed by Shadow IT

While employees may have good intentions when using shadow IT, they often lack a full understanding of the dangers involved. Working together, IT and end users can find solutions to mitigate risks that include the following:

- **Security gaps** – Using unsanctioned apps creates a potential opening for bad actors to inject malware or enter the system. For instance, when employees use apps without the knowledge of IT, they may be using programs with unpatched vulnerabilities.
- **Data loss** – Regular backups only include the sources known to the organization. When users store files outside the known network, they introduce the risk of losing that data without a recovery option. Additionally, storing and sharing sensitive information through risky apps increases the chance of data leaks.
- **Compliance issues** – Privacy regulations such as HIPAA include strict rules about the sharing, storage, and disposal of sensitive data. But when users store and share data using shadow IT, the organization cannot demonstrate compliance and may incur stiff penalties.

Combatting these risks requires a multifaceted approach. Consider the reasons that employees turn to using shadow IT. When approved apps prove cumbersome or lack necessary functionality, users look elsewhere. Likewise, if employees have not received adequate training in using sanctioned apps, they default to more comfortable sources.

When organizations keep communication lines open, they gain a better understanding of what their employees need and the ability to balance productivity with control. Then they can provide necessary training or conduct the research required to expand the list of sanctioned and controlled apps.



Control Risky App Usage by Blocking or Monitoring Apps

One helpful tool in monitoring risky app usage involves employing a cloud access security broker (CASB) such as Microsoft Defender for Cloud Apps. Formerly known as Microsoft Cloud App Security, Defender for Cloud Apps delivers critical visibility into all the cloud apps and services used throughout the organization.

Additionally, using Defender for Cloud Apps in conjunction with Microsoft Defender for Endpoints, organizations can block or monitor unapproved apps. That is, they can tag apps as sanctioned, unsanctioned, or monitored and create associated policies. They can also apply custom tags for alternative monitoring.

For instance, if users attempt to use an app tagged as "unsanctioned," Defender will block access to the app. On the other hand, if they attempt to use an app marked as "monitored," a warning message will display, but the user can bypass the block. They can also click a link to display a customized support page with details and alternatives.

Learn How to Use Microsoft Defender to Secure Your Cloud

Microsoft Defender for Cloud Apps plays a key role in the Microsoft 365 Defender security suite. By delivering visibility and control for cloud apps and services, it allows organizations to regain control of their cloud environment and shadow IT. This means increased security, as well reduced risk of compliance issues and data loss.

The compliance and security experts at Messaging Architects bring deep knowledge of Microsoft and other security and compliance technologies. They will help you choose and implement the tools and features you need to harness the power of the cloud while keeping critical data safe.