

ConnectWise Cloud Backup security incident and backup status

If you use ConnectWise Cloud Backup (formerly SkyKick) for Microsoft 365, you may have noticed tickets opened and resolved on your account this weekend. Those tickets were our response to a notice from ConnectWise that a security incident had occurred.

The notice included IP addresses associated with the presumed threat actors. We reviewed sign-in activity in client environments against those addresses, and our review found no evidence of unauthorized access.

As a precaution, we disabled the ConnectWise Cloud Backup application for clients under our management to mitigate the risk of further misuse of the vendor's compromised credential.

ConnectWise has not yet explained the cause of the breach. We have no information suggesting negligence on their part. Without an explanation to evaluate, though, we have decided to discontinue the product and migrate affected clients to a new backup platform.

WHAT THIS MEANS FOR YOUR BACKUPS

With the application disabled, Microsoft 365 backups are paused until the replacement platform is in place, or until ConnectWise provides reasonable assurance that resuming the service temporarily is safe. In the meantime, Microsoft's built-in recovery features remain available:

- Email: deleted messages move to Deleted Items. Once removed from there, they stay in Recoverable Items for a limited period, typically 14 to 30 days depending on your settings.
- OneDrive and SharePoint: deleted files move to the Recycle Bin, where they may be recovered for up to 93 days.

Items purged from these locations cannot be recovered. Please tell all staff not to empty Deleted Items, Recoverable Items or the Recycle Bin until we confirm the replacement backup is in place.

If you have questions about your specific Microsoft recovery settings, email me at this address and an engineer can provide a summary of your current settings. For organizations using disparate license types, please note that there may be different recovery settings for different users, and users for whom settings are requested must be individually specified in the email.

We will contact you again when the replacement solution is ready to deploy. We will also pass along any ConnectWise updates that we believe to be material to your organization's ongoing security. For anything else in the meantime, please reply to this email.

Sincerely,
Chris Harper
CSO, Sandbox Technologies, Inc.