CHECKLIST · SCAMS & SECURITY

ConnectWise's former SkyKick backup app was used to sign in to Microsoft 365 tenants. What IT providers and their clients should check

Published 19 October 2026. Read the full story, sources and any updates at
digitaladvisors.com.au/journal/connectwise-skykick-cloud-backup-microsoft-365-access/

- [ ] **Ask your IT provider whether your Microsoft 365 uses ConnectWise Cloud Backup, Cloud Management or SkyKick.** Include connections nobody uses any more, since ConnectWise says dormant ones need checking too.
- [ ] **Disable the apps in Microsoft Entra, but don't delete them.** In Enterprise applications, find each Application ID in ConnectWise's guide, starting with 506e08f9-6e9a-4da4-942b-a099a03644ae, and set sign-in to No.
- [ ] **Export the Entra audit and sign-in logs now.** Free-tier records are normally kept for seven days, and a licence upgrade won't bring back older history.
- [ ] **Search the sign-in logs for 144.172.64.128, 144.172.64.60 and 144.172.64.99.** Check service principal sign-ins as well as user sign-ins, from 13 October 2026.
- [ ] **Remove admin roles and app credentials you didn't grant, after recording them.** Look especially for Global Administrator held by a ConnectWise or SkyKick app, and for app secrets or certificates added since 13 October.
- [ ] **Check mailboxes for forwarding and inbox rules you didn't set.** ConnectWise also lists transport rules and delegated mailbox access.
- [ ] **Confirm in writing who is reviewing each tenant.** If a reseller supplied the service, make sure the guide reached the person who administers your tenant.
- [ ] **Leave the apps disabled until ConnectWise publishes reconnection instructions.** Meanwhile, check the date of your last successful backup so you know what isn't protected.

General information only, not legal, tax or financial advice. Check the full story and its sources before acting.