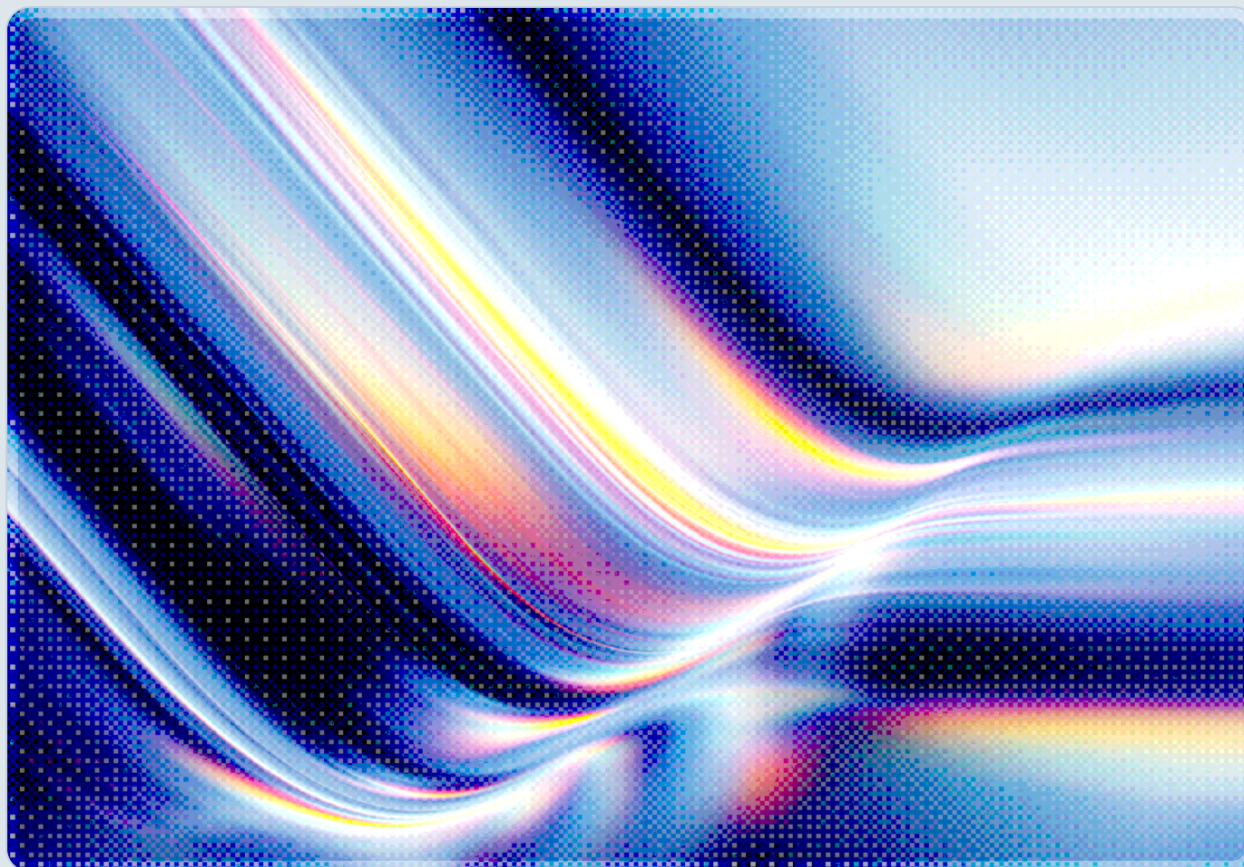


ConnectWise Cloud Backup: One Vendor App, 173 Tenants

Security Implications and Guidance

2026-10-17

 AI-assisted Rapid Research



CSAI

cloud
CSA security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Between 06:13 and 08:34 UTC on October 15, 2026, an unidentified actor used what reporting describes as a compromised vendor credential belonging to ConnectWise Cloud Backup (formerly SkyKick) to authenticate as that application into Microsoft 365 tenants of MSP partners and their customers [1][2]. The Hacker News reports 173 confirmed tenants [1]. Huntress's own write-up recorded 162 confirmed tenants as of 19:00 UTC on October 16 [2]. The figures differ between sources and time points, and the count may change again.

The incident is an application-identity compromise rather than a user-account compromise. Because the actor authenticated as the vendor's service principal, user passwords and MFA prompts would not have been part of the path, and Todyl's analysis describes the access as relying on permissions each customer had previously consented to [1][2]. Backup products commonly request broad read and write access to mail, files, Teams, and directory data, which makes the applications attractive targets.

In at least one tenant, Huntress observed the actor going beyond reading data: a related ConnectWise application granted itself the Global Administrator role, and client secrets valid until 2028 were added to two applications, including a security platform [2]. Huntress found no confirmed data exfiltration in the audit logs it reviewed, but notes that directory reads through Graph leave limited audit evidence [2]. ConnectWise has closed Cloud Backup application access and states it has found no evidence that partner backup data was compromised [1].

Defenders should treat this as an inventory and detection problem. Organizations should identify every third-party enterprise application holding tenant-wide permissions, review credentials and role assignments added since October 13, and be prepared to disable the affected applications until ConnectWise confirms credential rotation [2]. Disabling an application does not by itself end access already granted, because tokens already issued can remain valid for up to 90 minutes [1].

Background

ConnectWise Cloud Backup is the successor brand of SkyKick, a backup and migration product built for managed service providers (MSPs) [1]. MSPs install it into the Microsoft 365 tenants of their customers, and each installation involves an administrator consenting to a set of application permissions. Those

permissions are application-level rather than delegated, meaning the application can act without a signed-in user. The Hacker News and Huntress describe the granted scope as including read and write access to mail and attachments (including full mailbox access through Exchange Web Services), OneDrive and SharePoint files, Teams chats, and directory data [1][2].

The application's credential is held by the vendor, not by the customer. Public reporting indicates that a single vendor-held secret was sufficient to authenticate into many tenants, which suggests the number of affected organizations is bounded by the vendor's install base rather than by per-victim intrusion effort. This note does not establish whether one secret spans all customers, and the vendor's secret-management design has not been published.

According to Huntress, the activity was preceded by password spraying against law firm tenants on October 13 and 14, and on October 15 the actor began authenticating as the backup application from a single IP address, 144.172.64.128 [2]. Huntress lists the attacker's user agents as `Python-urllib/3.12` and `curl/7.88.1`, and contrasts them with legitimate ConnectWise traffic, which uses the `kiota-dotnet` SDK [2]. Microsoft reportedly detected broad successful service principal authentication on October 15, and Todyl independently confirmed unauthorized Graph authentication that relied on inherited consent [1]. How the vendor secret was obtained has not been publicly disclosed, and the relationship between the password spraying and the credential compromise is unestablished. Public reporting does not attribute the activity to a named actor.

Security Analysis

Anatomy of the access

Huntress reports that the actor moved through tenants in sorted GUID order, a few seconds apart, which suggests a script working from a target list rather than manual selection [1][2]. That pattern is consistent with the actor either holding a list of tenants where the application was installed or testing a broad tenant list and keeping those that succeeded. The source of any such list is not public. Access tokens issued to the application were reported to be valid for up to 90 minutes, even if the application is disabled in a tenant, which gives a window in which a single token can be used for mailbox, file, or directory reads without further authentication [1].

The reporting is consistent with the actor using the application's own permissions as the entry point and then probing for privilege escalation. In the tenant Huntress examined most closely, activity over roughly five minutes included a ConnectWise Cloud Management application assigning itself Global Administrator, and attempts to add credentials to applications [2]. Six changes succeeded and three

failed, with one certificate credential rejected [2]. A Python script using the urllib user agent performed the credential additions [1][2]. The added secrets, which expire in 2028 and sit on an MSP management tool and a security platform, would be expected to persist after the original application is disabled, and they sit on applications that administrators may not scrutinize [2]. Whether they survive depends on tenant configuration.

Why traditional controls did not apply

Controls that defend user identities do not apply to a service principal sign-in. Passwords, user-level MFA, and phishing-resistant authenticators are not part of an application's authentication, and Conditional Access for workload identities has a significant scope limit: Microsoft's documentation states that it applies to single-tenant service principals registered in the customer's own tenant, and that Microsoft and third-party SaaS applications, including multitenant apps, are not covered [4]. The ConnectWise application is a vendor-owned multitenant application, so that control cannot be used to restrict it. Huntress separately recommends checking whether any Conditional Access policy excludes the affected application, because broad exclusions for backup or management tools are common [2]. Microsoft's ID Protection documents risk detection for workload identities, including anomalous sign-in behavior, and states that detection covers multitenant and non-Microsoft SaaS applications [3]. Detections are available to all customers with limited reporting, while full details and risk-based Conditional Access require Workload Identities Premium licensing [3].

Visibility is the second gap. Service principal sign-ins appear in a distinct log category from interactive user sign-ins, and organizations that do not review that category will not see this activity [3]. Huntress cautions that directory reads through Graph may not appear in audit logs, so the absence of an audit record does not demonstrate that data was not read [2]. Customers therefore cannot currently demonstrate the absence of access from audit logs alone, even where no exfiltration was confirmed.

Vendor concentration and MSP exposure

The affected population is largely MSP partner tenants and their downstream customers [1]. An MSP tenant frequently holds delegated administrative relationships with many customers, such as delegated admin privileges or granular delegated admin privileges (GDAP), so a foothold there may extend further than the reported tenant count alone suggests. This is an inference and not a reported finding. Law firms were the apparent focus of the earlier password spraying [2], which is consistent with an interest in mailbox and document content, but the public record does not establish the actor's objective.

The incident follows a pattern CSA has documented in SaaS supply-chain breaches involving Salesloft, Gainsight, and Klue, where durable third-party OAuth trust, rather than a flaw in the victim's own environment, was the point of entry [5]. Here the platform is Microsoft 365 instead of Salesforce, and the credential is an application secret instead of a stolen refresh token, but the underlying exposure is the same: a vendor-held credential with standing, tenant-wide permissions.

Open questions

Several matters remain unresolved. The mechanism by which the vendor secret was exposed has not been published. The tenant count differs between sources and time points [1][2]. Whether data was read at scale, and by whom, is not established. ConnectWise has not published detailed indicators beyond those reported by Huntress, and the indicators that exist are weak: a single IP address and common user agents such as curl and urllib are easily changed, so their absence from logs should not be read as a clean result. Readers should expect revisions and should rely on the vendor's and Microsoft's advisories as they appear.

Recommendations

Immediate Actions

Organizations with ConnectWise Cloud Backup or SkyKick installed should find the application in Entra enterprise applications by its reported application ID, 506e08f9-6e9a-4da4-942b-a099a03644ae, and the related Cloud Management application, 24205314-2b89-4e07-a2a4-579e898a5640 [2]. Huntress advises disabling both applications rather than deleting them, which preserves configuration and logs, and not re-enabling them until ConnectWise confirms the credential has been reset [2]. Because tokens already issued can remain valid for up to 90 minutes after an application is disabled, disabling should be paired with the review steps below rather than treated as the end of the response [1].

Next, review all application and service principal credentials added since October 13, paying attention to secrets with distant expiry dates such as 2028, and review audit logs for directory role assignments made by ConnectWise or SkyKick applications [2]. Check sign-in logs, including the service principal category, for authentications from 144.172.64.128 and for the attacker user agents `Python-urllib/3.12` and `curl/7.88.1`, and check Conditional Access for exclusions covering these applications [2]. Do not hunt for `kiota-dotnet`, which Huntress identifies as the vendor's legitimate client [2]. Remove any unintended role grants and unexpected credentials, and treat role assignments, application credentials, mail-flow rules, and OAuth grants changed since October 13 as suspect until reviewed.

Short-Term Mitigations

Build an inventory of enterprise applications holding application permissions such as mail, files, or directory read and write, and rank them by blast radius. Alert on credential additions to service principals and on directory role assignments to applications. Because Conditional Access for workload identities does not cover vendor-owned multitenant applications such as this one, the controls that apply are application inventory, consent review, credential-change alerting, and disabling the service principal [4]. Where licensing permits, enable workload identity risk detection, which does cover multitenant applications [3]. Enable and retain Graph activity logging and service principal sign-in logs where available, and check licensing and retention limits, so that future investigations are not limited by the evidence gap described above. MSPs should additionally review delegated access relationships in customer tenants reachable from any tenant where the application was present.

Revisit least privilege with backup vendors. Ask whether the consented permissions are the minimum the product needs, whether write access is required, and whether the vendor supports customer-held credentials or certificate-based authentication with rotation. Update contracts and incident-notification terms so vendors disclose credential compromise on a defined timeline.

Strategic Considerations

CSA recommends treating third-party applications as identities with standing access, subject to the lifecycle governance applied to privileged human accounts: ownership, periodic recertification, expiry, and logging. These practices map to the identity and access management, supply chain management, and logging and monitoring domains of the AICM [6]. Vendor assurance reviews should ask how application secrets are generated, stored, and rotated, and whether a single secret spans all customers. Organizations should also plan for the case where a backup provider's access path is itself the compromised one, which argues for keeping recovery copies reachable independently of the primary vendor's application identity.

CSA Resource Alignment

CSA's threat intelligence report [ShinyHunters' OAuth Pivot: A Year of SaaS Supply-Chain Breaches](#) is the most closely related prior work. It analyzes the Salesloft, Gainsight, and Klue breaches and frames the "third-party OAuth trust gap" that the ConnectWise incident also illustrates [5]. Its guidance on inventorying and recertifying third-party grants is relevant to Microsoft 365 enterprise applications.

CSA's [AI Controls Matrix \(AICM\) v1.1](#) is CSA's primary controls framework, a superset of the Cloud Controls Matrix, and it covers the control domains this incident touches, notably identity and access management, supply chain management, and logging and monitoring [6]. CSA's STAR program is also relevant to vendor assurance more generally, and customers can use it as one input when evaluating a vendor's security posture [7]. The specific questions on secret management and breach notification raised above should be asked of vendors directly.

References

- [1] The Hacker News. "[Hackers Use Compromised ConnectWise Credential to Sign In to 173 Microsoft 365 Tenants](#)." The Hacker News, October 17, 2026.
- [2] Huntress. "[ConnectWise \(SkyKick\) Vendor Credentials Abused in M365 Attacks](#)." Huntress, October 2026.
- [3] Microsoft. "[Securing workload identities with Microsoft Entra ID Protection](#)." Microsoft Learn, updated March 26, 2026. Accessed October 17, 2026.
- [4] Microsoft. "[Conditional Access for workload identities](#)." Microsoft Learn, updated May 18, 2026. Accessed October 17, 2026.
- [5] Cloud Security Alliance. "[ShinyHunters' OAuth Pivot: A Year of SaaS Supply-Chain Breaches](#)." CSA Labs, July 16, 2026.
- [6] Cloud Security Alliance. "[AI Controls Matrix v1.1](#)." CSA, June 22, 2026.
- [7] Cloud Security Alliance. "[STAR Program](#)." CSA. Accessed October 17, 2026.