SKYKICK / MICROSOFT 365

Disable the connection. Follow the access.

ORIGINAL CONNECTION



Disabled

Containment step

ACCESS ADDED ELSEWHERE



Investigate

Separate credentials or roles

Vendor containment is not tenant clearance.

Incident response guidance, not proof every tenant was affected.

Sources: ConnectWise, Huntress, Microsoft

Checked Oct 19, 2026

SKYKICK / MICROSOFT 365

What was reported?

CLOUD BACKUP

Unauthorized app sign-ins

ONE CUSTOMER TENANT

Credentials added to two other trusted apps

Huntress reporting; separate observations.
These are not one continuous attack timeline.

SKYKICK / MICROSOFT 365

Check three places.

01 **Sign-ins**
Which app authenticated?

02 **Directory changes**
What access was added?

03 **Resource activity**
What was touched?

Build an evidence ladder.
One record does not prove the next.

Sources: ConnectWise, Huntress, Microsoft
Checked Oct 19, 2026

SKYKICK / MICROSOFT 365

An empty search needs a coverage check.

01 **Records available**
The source contains records.

02 **No matches found**
The search returned no matches.

03 **Records missing**
Evidence may be unavailable.

Record source, time range, tenant, and gaps.
An empty search is not an all-clear.

Sources: ConnectWise, Huntress, Microsoft
Checked Oct 19, 2026

SKYKICK / MICROSOFT 365

One MSP review does not clear every customer.



Assign an owner and status to each tenant, including dormant connections.

Each tenant needs its own evidence and decisions.

Sources: ConnectWise, Huntress, Microsoft

Checked Oct 19, 2026

SKYKICK / MICROSOFT 365

Contain. Investigate. Restore deliberately.

01 Keep affected connections disabled under current guidance.

02 Remove confirmed unauthorized access and follow its use.

03 Check the last recovery point and restoration path.

Full response guide + tenant worksheet

deceptioncheck.ai/research

Sources: ConnectWise, Huntress, Microsoft

Checked Oct 19, 2026