CLAUDE CO-WORK
WHY IT CAN BE A SECURITY RISK
A SIMPLE, HIGH-LEVEL VIEW

1. SECURITY TOOLS MAY NOT SEE INSIDE IT

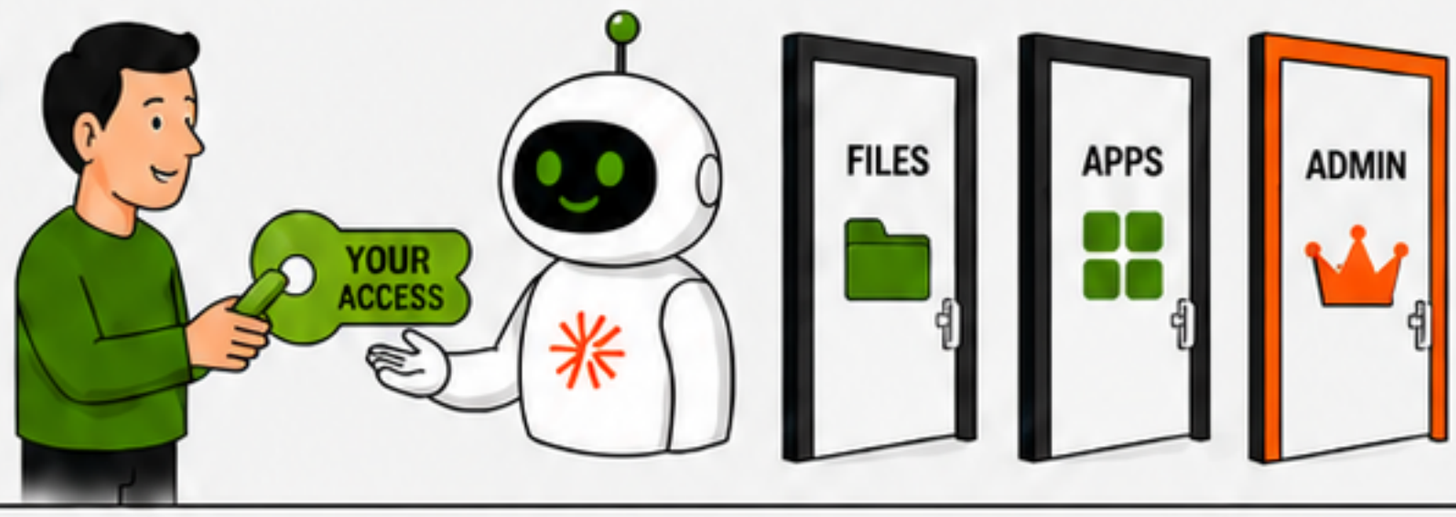
Claude Co-work runs in its own workspace, like a room inside a room.

Your security tools may not fully see or control what happens in there.

2. IT CAN USE YOUR ACCESS

If it is signed in as you, it can use the same permissions you have.

If you are an admin, it may reach admin-only apps, files, settings, and data too.

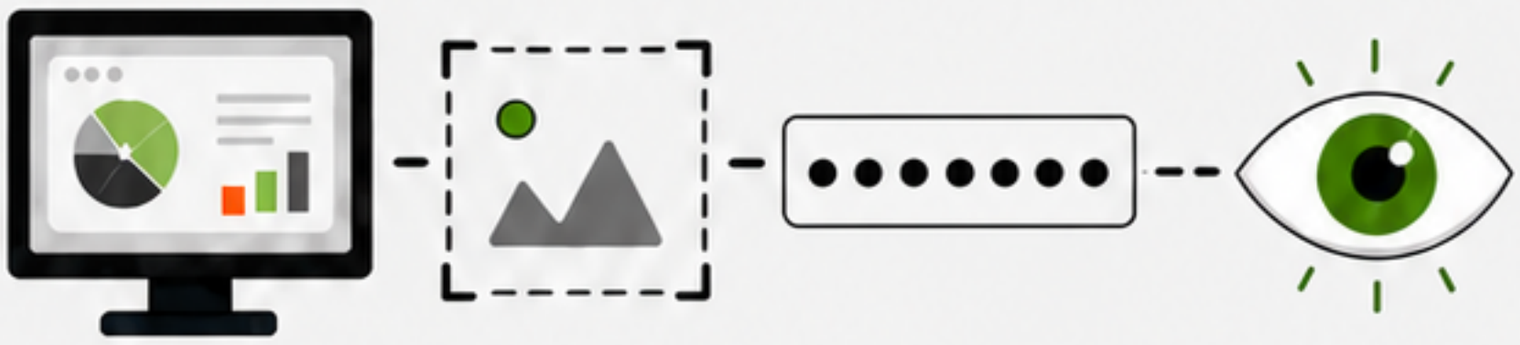


3. IT CAN ACT INSIDE MICROSOFT 365

If it connects to your Microsoft 365 account, it may read company information and take actions for email, files, chat, and settings on your behalf.

4. IT MAY SEE SENSITIVE THINGS

To help you, it may look at screens, take screenshots, and capture passwords or other secrets that appear on screen.



5. OLD SIGN-INS CAN STILL BE RISKY

If an employee leaves but Claude is still signed in, old sessions or tokens could still be misused later.

WHAT THIS MEANS

If a tool can see what you see and act like you act, one unsafe account can become a much bigger problem.

SCHEDULE YOUR AI READINESS ASSESSMENT

See where AI tools may be exposing your users, tenant, and data.

https://www.integramsp.com/aiready

Questions? sales@integraMSP.com | 214-705-2008

Good governance starts with knowing what is already in play.

IntegraMSP
PARTNERSHIPS BUILT ON INTEGRITY