

GHOSTAPPROVAL

The AI knew what it was editing.
The human didn't.

SWIPE →

WHAT USERS SAW

Edit project_settings.json?



WHAT THE SYSTEM KNEW

~/.ssh/authorized_keys



**The approval dialog
wasn't wrong.**

It was incomplete.



6 VENDORS TESTED



AWS

Fixed



Cursor

Fixed



Google

Fixed



Anthropic

Warning only



Augment

Unpatched



Windsurf

Writes before approval

Human-in-the-loop only works when:

WHAT IS SHOWN

=

WHAT IS EXECUTED

The loop isn't the control.

The dialog's honesty is.

rack2cloud.com | Follow The Architect for more