The Cloud Permissions Firewall for AI Agents

STOP MACHINE-SPEED ATTACKS BY ENFORCING LEAST PRIVILEGE – AUTOMATICALLY

Sonrai's Cloud Permissions Firewall secures every AI agent, human, and machine identity by enforcing default-deny permissions in real time – preventing AI agents from going rogue or misusing access.

THE PROBLEM: AI HAS BROKEN DETECTION-BASED SECURITY

AI agents operate at machine speed. They can escalate privileges, move laterally, and exfiltrate sensitive data in minutes. They can test thousands of permission paths instantly making them relentlessly persistent. Traditional human-paced detection tools simply cannot react fast enough.

27 SECONDS

Fastest recorded lateral movement in modern cloud breaches

4 MINUTES

Documented time to data exfiltration in machine-speed attacks

4.5 TIMES

Higher breach risk when AI identities are granted excessive permissions

92 PERCENT

Cloud identities granted privileged permissions they never use

THE SOLUTION: CLOUD PERMISSIONS FIREWALL FOR AI AGENTS

Sonrai's Cloud Permissions Firewall stops AI-assisted attacks by enforcing default-deny permissions across every AI agent, human, and machine identity. Rather than detecting misuse, Sonrai removes it. Even if an agent is compromised or manipulated, it lacks the permissions to do damage.

HOW SONRAI SECURES AI AGENTS

1 AI AGENT DISCOVERY & IDENTITY MAPPING

Automatically identifies AI agent identities and links them to the humans who grant their permissions – exposing hidden privilege escalation paths.

2 DEFAULT-DENY ENFORCEMENT VIA CLOUD-NATIVE POLICIES

Applies automated guardrails that block all privileged actions unless explicitly approved – stopping unauthorized agent behavior before damage.

3 ONE-CLICK REMOVAL OF UNUSED PERMISSIONS

Instantly blocks unused permissions that attackers and agents exploit for lateral movement.

4 PERMISSIONS ON DEMAND (POD)

When agents need new permissions, owners can approve time-bound access via Slack or Teams – maintaining security without slowing development.

A Complete Identity Security Platform for AI, Humans and Machines

Stop AI agents from becoming your fastest attackers.
You cannot detect your way out of an AI-driven breach. Protect your cloud with automated least privilege enforcement – the only viable defense in a machine-speed threat environment.

Book a demo Learn more