

Strangers in your *home*

A NORTHLIGHT PICTURES PRODUCTION A FILM BY JONAS EIKEN
"STRANGERS IN YOUR HOME" LARS EKLUND ELLA NORDSTRÖM ADAM LUNDGREN
DIRECTOR OF PHOTOGRAPHY MATTIAS LINDGREN PRODUCTION DESIGN SOFIA KARLSSON
EDITED BY ERIK DAHL MUSIC BY JOHAN SÖDERQVIST
WRITTEN BY JONAS EIKEN PRODUCED BY MIKAEL BERG DIRECTED BY JONAS EIKEN





Controlling access of Claude & Co

Runtime governance for AI agents

Johannes Keienburg · Co-Founder & CEO Cakewalk Security

Claude Code Munich · June 10, 2026

What's your guess?

github-mcp-tools.json


Raw

```
1  [
2    {
3      "inputSchema": {
4        "json": {
5          "properties": {
6            "body": {
7              "description": "Comment content",
8              "type": "string"
9            },
10           "issue_number": {
11             "description": "Issue number to comment on",
12             "type": "number"
13           },
14           "owner": {
15             "description": "Repository owner",
16             "type": "string"
17           },
18           "repo": {
19             "description": "Repository name",
20             "type": "string"
21           }
22         },
23         "required": [
24           "owner",
25           "repo",
26           "issue_number",
27           "body"
28         ],
29         "type": "object"
30       }
31     },
32     "name": "add_issue_comment",
33     "description": "Add a comment to a specific issue in a GitHub repository."
34   },
35   {
36     "inputSchema": {
```



GitHub: 51 tools

All connections > PostHog

 **PostHog**
How engineers build better products

OVERVIEW USERS SESSIONS **TOOLS**

Q Search...

<input type="checkbox"/>	Name	Action type	Description
<input type="checkbox"/>	action-create	External	Create a new action in the project. Actions define reusable event triggers based on page views, clicks, form sub...
<input type="checkbox"/>	action-delete	Destruc...	Delete an action by ID (soft delete - marks as deleted). The action will no longer appear in lists but historical dat...
<input type="checkbox"/>	action-get	External	Get a specific action by ID. Returns the action configuration including all steps and their trigger conditions.
<input type="checkbox"/>	action-update	External	Update an existing action by ID. Can update name, description, steps, tags, and Slack notification settings.
<input type="checkbox"/>	actions-get-all	External	Get actions in the project. Actions are reusable event definitions that can combine multiple trigger conditions (p...
<input type="checkbox"/>	activity-log-list	External	List recent activity log entries for the project. Shows who did what and when — feature flag changes, dashboard...
<input type="checkbox"/>	advanced-activity-logs-filters	External	Get the available filter options for activity logs — scopes, activity types, and users that have logged activity. Use...
<input type="checkbox"/>	advanced-activity-logs-list	External	List activity log entries with advanced filtering, sorting, and field-level diffs. Supports filtering by scope, activity ...
<input type="checkbox"/>	alert-create	External	Create a new alert on an insight. Alerts can use either threshold-based conditions or anomaly detection. For thre...
<input type="checkbox"/>	alert-delete	Destruc...	Delete an alert by ID. This permanently removes the alert and all its check history. Subscribed users will no longe...
<input type="checkbox"/>	alert-get	External	Get a specific alert by ID. Returns the full alert configuration including check results, threshold settings, detector...
<input type="checkbox"/>	alert-simulate	External	Run an anomaly detector on an insight's historical data without creating any alert or check records. Use this to ...
<input type="checkbox"/>	alert-update	External	Update an existing alert by ID. Can update name, threshold, condition, config, detector_config, subscribed user...
<input type="checkbox"/>	alerts-list	External	List all insight alerts in the project. Returns alerts with their current state, threshold or detector configuration, ti...

411 tools in this view

PostHog: 411 tools

Q Search...

11

<input type="checkbox"/>	Name	Action type	Description
<input type="checkbox"/>	create_attachment	Write	Deprecated fallback for tiny files only. Accepts base64 file content and uploads it through the MCP worker, whic...
<input type="checkbox"/>	create_attachment_from_upload	Write	Link an already-uploaded Linear assetURL to an existing issue as an attachment. Use this only after: 1. prepare_...
<input type="checkbox"/>	create_issue_label	Write	Create a new Linear issue label
<input type="checkbox"/>	delete_attachment	Destruct...	Delete an attachment by ID
<input type="checkbox"/>	delete_comment	Destruct...	Delete a Linear comment. Inline description comments (those with non-null "quotedText") anchor a mark in the ..
<input type="checkbox"/>	delete_customer	Destruct...	Delete a customer in Linear
<input type="checkbox"/>	delete_customer_need	Destruct...	Archive a customer need in Linear
<input type="checkbox"/>	extract_images	External	Extract and fetch images from markdown content. Use this to view screenshots, diagrams, or other images embed...
<input type="checkbox"/>	get_attachment	Read	Retrieve an attachment's content by ID.
<input type="checkbox"/>	get_diff	Read	Exact lookup for a Linear diff. Use with review URLs, GitHub PR URLs, Linear full identifiers, UUIDs, or slugs.
<input type="checkbox"/>	get_diff_threads	External	Exact lookup for diff threads. Use with review URLs, GitHub PR URLs, Linear full identifiers, UUIDs, or slugs.
<input type="checkbox"/>	get_document	Read	Retrieve a Linear document by ID or slug
<input type="checkbox"/>	get_issue	Read	Retrieve detailed information about an issue by ID, including attachments and git branch name
<input type="checkbox"/>	get_issue_status	Read	Retrieve detailed information about an issue status in Linear by name or ID.
<input type="checkbox"/>	get_milestone	Read	Retrieve details of a specific milestone by ID or name
<input type="checkbox"/>	get_project	Read	Retrieve details of a specific project in Linear
<input type="checkbox"/>	get_team	Read	Retrieve details of a specific Linear team
<input type="checkbox"/>	get_user	Read	Retrieve details of a specific Linear user
<input type="checkbox"/>	list_comments	Read	List comments on a Linear issue, project, initiative, document, or project milestone. Provide exactly one of "issue..."
<input type="checkbox"/>	list_customers	Read	List customers in the user's Linear workspace
<input type="checkbox"/>	list_cycles	Read	Retrieve cycles for a specific Linear team
<input type="checkbox"/>	list_diffs	Read	List Linear diff pull requests visible to the authenticated user
<input type="checkbox"/>	list_documents	Read	List documents in the user's Linear workspace
<input type="checkbox"/>	list_issue_labels	Read	List available issue labels in a Linear workspace or team
<input type="checkbox"/>	list_issue_statuses	Read	List available issue statuses in a Linear team
<input type="checkbox"/>	list_issues	Read	List issues in the user's Linear workspace. For my issues, use "me" as the assignee. Use "null" for no assignees.
<input type="checkbox"/>	list_milestones	Read	List all milestones in a Linear project
<input type="checkbox"/>	list_project_labels	Read	List available project labels in the Linear workspace
<input type="checkbox"/>	list_projects	Read	List projects in the user's Linear workspace
<input type="checkbox"/>	list_teams	Read	List teams in the user's Linear workspace
<input type="checkbox"/>	list_users	Read	Retrieve users in the Linear workspace
<input type="checkbox"/>	prepare_attachment_upload	Write	Prepare a direct Linear file upload for an existing issue. Workflow: 1. Call this tool with issue, filename, contentTy...
<input type="checkbox"/>	save_comment	Write	Create or update a comment on a Linear issue, project, initiative, document, or project milestone. If "id" is provi...
<input type="checkbox"/>	save_customer	Write	Create or update a Linear customer. If "id" is provided, updates the existing customer; otherwise creates a new ...
<input type="checkbox"/>	save_customer_need	Write	Create or update a customer need (request) in Linear. If "id" is provided, updates the existing need; otherwise c...
<input type="checkbox"/>	save_document	Write	Create or update a Linear document. If "id" is provided, updates the existing document; otherwise creates a ne...
<input type="checkbox"/>	save_issue	Write	Create or update a Linear issue. If "id" is provided, updates the existing issue; otherwise creates a new one. Wh...
<input type="checkbox"/>	save_milestone	Write	Create or update a milestone in a Linear project. If "id" is provided, updates the existing milestone; otherwise cr...
<input type="checkbox"/>	save_project	Write	Create or update a Linear project. If "id" is provided, updates the existing project; otherwise creates a new one...
<input type="checkbox"/>	search_documentation	Read	Search Linear's documentation to learn about features and usage

40 tools in this view



Linear:

40 tools

Zero access governance



Static access

Broad permissions

No central visibility



Agentic Infrastructure.

▲ Vercel

11947

Framer

Enterprise needs.
Startup speeds.

OUTFRONT

14'x48'

In Memoriam
The Billable Hour

In lieu of flowers, send contracts to crosby.ai

CROSBY
The First AI Law Firm

001008

Agents trace.
You draw.

Graphite

SAN FRANCISCO · MAY 2026

LangChain

Track your agents like your macros

Monitor agents with
LangSmith

ONE WAY



Agents work where you don't.

Retool

Pay here
Pay here
1/2
36100004

04 /

How Vercel got breached via an agent



A screenshot of a Vercel security bulletin page. The page has a white background with a light gray header. The header includes the Vercel logo, navigation links for Products, Resources, Solutions, Enterprise, and Pricing, and a search bar for the Knowledge Base. The main content area is framed by a thin gray border. At the top of this area, there is a breadcrumb trail: "← Knowledge Base / Security Bulletin". The main heading is "Vercel April 2026 security incident" in a large, bold, black font. Below the heading, there is a paragraph: "We've identified a security incident that involved unauthorized access to certain internal Vercel systems." This is followed by a small icon of a person and the text "Security Team". Below that, there are three links: "Copy URL", "Copy page", and "Ask AI about this page". Underneath these links, it says "4 min read" and "Last updated April 24, 2026". There is a text input field with the placeholder "Enter your email to subscribe for updates" and a right-pointing arrow button. At the bottom of the page, there is a paragraph of text: "We've identified a security incident that involved unauthorized access to certain internal Vercel systems. We are actively investigating, and we have engaged incident response experts to help investigate and remediate. We have notified law enforcement and will update this page as the investigation progresses." Below this paragraph, it says "In this bulletin:".

Employee gives Context.ai "Allow All" on Google Workspace

Infostealer at Context.ai exposes stored OAuth grants

Attacker rides the grant into Vercel → internal env → keys, tokens, credentials

Four runtime governance approaches



Protocol Gateway

NETWORK LAYER

Sees every tool call. Cloud + self-hosted.



SDK Instrumentation

AGENT RUNTIME

Deepest context, but per-framework and bypassable.



Kernel

OPERATING SYSTEM

A backstop for forbidden actions. Limited context.



Vendor App Integration

INSIDE EACH APP

Only where the vendor builds the hooks.

At a Glance



Same problem, four layers, different tradeoffs

	Protocol Gateway	SDK Instrumentation	Kernel	Vendor App Integration
Where it sits	Protocol layer	Runtime	Operating system	Vendor app
How hard to circumvent	High	Medium	High	Depends on vendor
Context awareness	Medium	High	Low	Depends on vendor
Integration effort	Low	Medium	None	Low (if available)
Self-hosted agents	✓	✓	✓	✓
Cloud agents	✓	✗	✗	✓
Meets the AARM standard	✓	✓	✗	Only if vendor provides full hooks
Third-party dependency	Not needed	Required	Not needed	Required
Best for	<i>Any agent that connects to tools via MCP or standard protocols</i>	<i>Self-hosted agents where you control the code</i>	<i>Backstop layer for forbidden actions</i>	<i>Cloud agents where the vendor provides governance hooks</i>



Lucy Chen

Marketing | Manager

HubSpot

Mailchimp

Google Workspace

Canva

CLICK A PROMPT TO RUN

Send a newsletter campaign

Access customer payment records

Query production server logs



Joe Park

Engineering | Senior

GitHub

AWS

Datadog

PostgreSQL

CLICK A PROMPT TO RUN

Send a newsletter campaign

Access customer payment records

Query production server logs



Angela Torres

Sales | Lead

Salesforce

Gong

HubSpot

Stripe

CLICK A PROMPT TO RUN

Send a newsletter campaign

Access customer payment records

Query production server logs

USERS



Lucy Chen



Joe Park



Angela Torres

AI AGENTS



Cursor



Claude Desktop



Windsurf



ChatGPT

CAKEWALK GATEWAY



Cakewalk Gateway

APPS



HubSpot



AWS



Google Workspace



GitHub



Stripe



Salesforce

policy_evaluation_engine

ACTION TYPE

READ

USER CONTEXT

Angela Torres (Sales / Lead)

APP CONTEXT

AWS | Production | High Risk

POLICY MATCH

"Sales has no access to production infrastructure."

OUTCOME

⊗ DENY

The policy layer between agents & apps



Policy Engine

Per-action rules in real time. Reads approve, writes escalate, destructive deny.



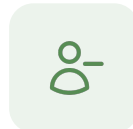
Credential Mediation

Agents never see real tokens. Held in the vault, injected per call.



Least Privilege

Just-in-time access, scoped to the task, revoked when the work is done.



Identity-Linked Lifecycle

Offboard the human and the agents go too. Every call traces to a person.



Agent Discovery

Every agent, one catalog, one kill-switch. Shadow AI becomes sanctioned AI.

Works across cloud, local, self-hosted and multi-agent setups - **one gateway for all of them.**



Governance and autonomy.
Not either / or.