THE CYBER TOOLCHAIN

NO. 012

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 11, 2026 · EVERY WEEKDAY

The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // **CONTENTS** SHOW 15 tools

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Reverse Engineering

jadx ⓘ v1.5.6 NOTES ↗

Dex to Java decompiler

jadx v1.5.6 adds graph views with code pane sync, a call graph library, and resource tree improvements.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.5.6 https://github.com/skylot/jadx.git
# already have the repo? check out this version:
$ git checkout v1.5.6
```

- Adds graph views with code pane synchronization in the GUI for visual code flow analysis.
- New call graph module/library enables programmatic traversal of method call relationships.
- Collapses single-child directory chains in the resource tree for cleaner navigation.
- Adds 'Copy Reference' option to the context menu for quick symbol referencing.
- Supports pasting file lists directly into the file chooser dialog.

+1 more

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Cloudflare ⓘ

Improving Smart Tiered Cache for Public Cloud Regions (2026-07-10) BLOG ↗

Cloudflare Blog is an official publication sharing updates, technical insights, and announcements about Cloudflare's internet security, performance, and networking products and services.

Cloudflare Smart Tiered Cache now supports cloud region hints for AWS, GCP, Azure, and Oracle Cloud anycast origins.

└──▷ HOW TO FIND IT

Set a region hint for an anycast AWS origin so Smart Tiered Cache routes through the optimal upper tier instead of hairpinning across continents.

> 📍 In the Cloudflare dashboard, go to Caching › Tiered Cache › Origin Configuration. Find your anycast origin IP, click the edit icon, select "Set Region Hint", and choose your region (e.g., aws:us-east-1). Save to apply.

- Adds cloud region hint configuration for anycast origins, letting Smart Tiered Cache select optimal upper tiers for origins on AWS, GCP, Azure, and Oracle Cloud.
- New Origin Configuration table in the dashboard (Caching > Tiered Cache > Origin Configuration) enables per-IP region hint assignment or bulk editing of all origin IPs at once.
- Supports region hint management via Cloudflare API and Terraform for infrastructure-as-code workflows.
- Introduces anycast origin detection using speed-of-light latency checks across multiple global checkpoint data centers.
- Automatically refreshes cloud provider IP range mappings every few hours and upper-tier probe data every 15 minutes, with geographic fallback for regions lacking probe data.

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Docker Compose ⓘ v5.3.0 2 RELEASES · 2026-06-23 → 2026-07-02

NOTES ↗ LATEST STABLE

Define and run multi-container applications with Docker

Docker Compose v5.3.0 adds native support for pre-start init containers.

└──▷ GET THIS VERSION

```
$ git clone --branch v5.3.0 https://github.com/docker/compose.git
# already have the repo? check out this version:
$ git checkout v5.3.0
```

└──▷ USE IT

Run a setup task (e.g., DB migration) in an init container that must succeed before your app service starts.

yaml

```yaml
services:
  app:
    image: myapp:latest
    depends_on:
      init-migrate:
        condition: service_completed_successfully
  init-migrate:
    image: myapp:latest
    command: ["python", "manage.py", "migrate"]
    x-init: true
```

› Supports pre-start init containers, allowing services to declare initialization containers that run and complete before the main service starts.

▾ 1 more release in this issue · 2026-06-23 → 2026-07-02

v5.2.0 NOTES ↗ STABLE

Docker Compose v5.2.0 introduces a new reconciliation algorithm and a rawsetenv message type for provider plugins.

└──▷ GET THIS VERSION

```
$ git clone --branch v5.2.0 https://github.com/docker/compose.git
# already have the repo? check out this version:
$ git checkout v5.2.0
```

- New reconciliation algorithm aligns observed state with expected state more accurately during `docker compose up` and related operations.
- Adds `rawsetenv` message type for provider plugins, enabling plugins to set environment variables without shell interpolation.

WAS THIS USEFUL? 👍 👎

◆ Runtime Security

Docker Sandboxes

v0.35.0

3 RELEASES · 2026-06-17 → 2026-07-10

NOTES ↗ LATEST STABLE

Docker Sandboxes v0.35.0 adds SOCKS5 proxy support, policy inspection/check commands, secret import, and a daemon management CLI.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.35.0 https://github.com/docker/sbx-releases.git
# already have the repo? check out this version:
$ git checkout v0.35.0
```

└──▷ TRY IT

Before running an agent task, verify that the current policy permits a specific outbound connection — catch misconfigurations without launching the full sandbox.

```
$ sbx policy check network --host api.example.com --port 443
```

Route all sandbox egress through a corporate SOCKS5 proxy (with credentials) so sandbox traffic flows through your org's inspection infrastructure.

```
$ DOCKER_SANDBOXES_PROXY=socks5://proxyuser:proxypass@proxy.corp.example.com:1080 DOCKER_SANDBOXES_NO_PROXY=localhost,127.0.0.1 sbx run
```

Migrate host env-var credentials (e.g. API keys) into the keychain so they are explicitly managed rather than auto-injected at runtime.

```
$ sbx secret import
```

- Adds SOCKS5 upstream-proxy transport (`socks5://` / `socks5h://`) for sandbox egress via `DOCKER_SANDBOXES_PROXY` , `HTTP_PROXY` , or `HTTPS_PROXY` , with optional auth and `DOCKER_SANDBOXES_NO_PROXY` exclusions.
- New `sbx policy inspect` command to examine policy details.

› New `sbx policy check network` command to test whether the current policy would allow a network access request before executing.

› Revamped `sbx policy ls` with `--wide`, `--source`, and `--decision` filters for concise policy listing.

› New `sbx secret import` imports credential env vars into the keychain; `sbx secret ls` now flags env-only and OAuth-shadowed entries. Host env vars no longer auto-inject at runtime — migration required.

+10 more

└──▷ **BREAKING ON UPGRADE**

! Host env vars no longer auto-inject at runtime — use `sbx secret import` to migrate existing env-var-based secrets.

! `sbx rm` now won't delete an active session unless `--force` is passed.

! Installation is blocked on Windows versions older than Windows 11.

▾ **2 more releases in this issue** · 2026-06-17 → 2026-07-10

v0.34.0 NOTES ↗ STABLE

Docker Sandboxes v0.34.0 adds a native SSH endpoint, kit source allowlisting, OCI v2 streaming, and a new onboarding command.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.34.0 https://github.com/docker/sbx-releases.git
# already have the repo? check out this version:
$ git checkout v0.34.0
```

└──▷ **TRY IT**

Enable the experimental SSH endpoint so agents or operators can shell directly into a running sandbox without a separate proxy.

```
$ sbx settings set feature.ssh true
```

Connect an interactive shell to a named sandbox over the native SSH endpoint once feature.ssh is enabled.

```
$ ssh <sandbox-name>@127.0.0.1 -p 2222
```

Allow kit installs from a private registry or Git source in addition to Docker Hub, to avoid the new allowlist breaking change.

```
$ sbx settings set kit.allowedSources ghcr.io/myorg/
```

- New experimental native SSH endpoint in sandboxd: connect with `ssh <sandbox-name>@127.0.0.1 -p 2222` (publickey auth, connect-to-create, interactive shell and exec).
- New experimental `sbx setup` command imports agent credentials from environment variables for smoother first-time onboarding.
- Adds OCI v2 kit artifact streaming that decompresses layers once to a cache directory and uses seek-based random access, reducing memory pressure during kit reads.
- Restricts kit installs to an allowlist of sources (default: Docker Hub only); installing from other registries or Git URLs now fails unless explicitly permitted — `breaking change`.
- Renames `sbx policy set-default` to `sbx policy init`; old name kept as a hidden deprecated alias.

`+1 more`

└──▷ BREAKING ON UPGRADE

- **!** Kit installs are restricted to an allowlist of sources defaulting to Docker Hub (`docker.io/`) only; installing a kit from another registry or a Git URL fails until you add its prefix with `sbx settings set kit.allowedSources`.
- **!** The `sbx policy set-default` command is renamed to `sbx policy init` (the old name still works as a hidden deprecated alias, but is deprecated).

`v0.33.0` `NOTES ↗` `STABLE`

sbx v0.33.0 adds named sandbox identity, DNS-gated network policy, wildcard secrets, and Cursor OAuth support.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.33.0 https://github.com/docker/sbx-releases.git
# already have the repo? check out this version:
$ git checkout v0.33.0
```

└──▷ TRY IT

Run two independent Claude Code sandboxes in the same workspace — useful when parallelising agent tasks without them colliding.

```
$ sbx run --name feature-a claude && sbx run --name feature-b
claude
```

Re-attach to a named sandbox from a different directory without specifying an agent, useful when returning to a long-running session.

```
$ sbx run --name feature-a
```

Grant a custom secret to all subdomains of an internal service using wildcard host patterns.

```
$ sbx secret set-custom --host '*.internal.corp' --host
'**.api.internal.corp' MY_API_TOKEN
```

- New `--name` flag for `sbx run` identifies a sandbox independently of the working directory, enabling multiple named sandboxes in the same workspace and re-attachment from any directory.
- `sbx ls --json` now reports a stable per-sandbox `id` field for scripting and automation.
- Sandbox DNS resolution is now gated on network policy, closing a DNS-based data-exfiltration channel (CVE-2026-12039); loopback names remain exempt.
- Outgoing ICMP from sandboxes is now blocked persistently across daemon restarts (CVE-2026-12539).
- `sbx secret set-custom --host` and `serviceDomains` in kits now accept wildcard host patterns (`*` for one label, `**` for any number) and are repeatable, allowing one secret to cover multiple subdomains.

+8 more

BREAKING ON UPGRADE

- The `sbx run <name>` positional argument form for re-attaching to an existing sandbox now prints a deprecation warning; the positional argument for `sbx run` is expected to be an agent (e.g. `claude`, `codex`), not a sandbox name, and the old positional-name form will be removed in a future release.
- `sbx run --name` no longer auto-creates numbered sibling sandboxes when a same-named sandbox exists.

! `sbx create` now errors when run without arguments instead of proceeding.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Microsoft Sysinternals ⓘ

LiveKd v5.65, ProcDump v12.01, and ZoomIt v12.11 (2026-07-09) BLOG ↗

Microsoft Sysinternals is a suite of advanced Windows system utilities for troubleshooting, monitoring, and diagnosing operating system internals, processes, and security issues.

LiveKd 5.65 restricts dump file access to admins; ZoomIt 11.11 adds JPEG and WEBP snip format support.

- LiveKd now protects generated kernel dump files from being read by non-admin users.
- ZoomIt adds JPEG and WEBP format support for snip captures.

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Datadog Stratus Red Team ⓘ v2.34.0 NOTES ↗ CODE ↗

Granular, Actionable Adversary Emulation for the Cloud

Stratus Red Team v2.34.0 adds Azure App Service credential harvesting, a controllable logger API, and a threat-intel coverage mapping skill.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.34.0 https://github.com/DataDog/stratus-red-team.git
# already have the repo? check out this version:
$ git checkout v2.34.0
```

└──▷ USE IT

Route all Stratus library log output through your own zap logger instead of the default stdout handler — useful when embedding Stratus in a larger tool.

go

```
import (
    "log/slog"
    stratuslog "github.com/datadog/stratus-red-team/v2/pkg/stratus/log"
    "go.uber.org/zap"
    "go.uber.org/zap/exp/zapslog"
)

func init() {
    zapLogger, _ := zap.NewProduction()
    handler := zapslog.NewHandler(zapLogger.Core(), zapslog.WithCaller(false))
    stratuslog.SetLogger(slog.New(handler))
}
```

- New Azure attack technique: Retrieve App Service Publishing Credentials (`azure.credential-access.app-service-publishing-credentials`).
- New `pkg/stratus/log` package exposes a controllable logger, letting library embedders route Stratus log output through any `slog.Handler` (e.g., zap, logrus).
- New `map-threat-intel-coverage` agent skill fetches a threat-intelligence report, extracts cloud TTPs, classifies each against existing Stratus Red Team coverage, and drafts GitHub issues for gaps.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Compliance Automation & Trust Management

Vanta ⓘ June 2026 NOTES ↗

Vanta June 2026 adds audit commenting, MCP expansion, AIUC-1 pilot, CrowdStrike CSPM, Twilio integration, and 20 new privacy MCP tools.

└──▷ HOW TO FIND IT

Discuss a specific control gap with your auditor in-context during an audit, without leaving Vanta.

> 📍 In the Vanta console, go to Audits › [your audit] › Controls, click a control row, select 'Comments', type your message, and @mention your auditor to notify them directly.

Connect a custom or internal MCP-capable tool to Vanta's MCP to automate compliance workflows without waiting for manual allowlisting.

> 📍 In the Vanta console, go to Integrations › MCP, copy the MCP connection URL, paste it into your MCP-capable tool. If the redirect URL is not Vanta-owned, acknowledge the warning banner to proceed.

Ingest CrowdStrike CSPM cloud misconfiguration findings into Vanta to track remediation SLAs and generate audit evidence.

> 📍 In the Vanta console, go to Integrations › CrowdStrike, select 'Add Connection', choose your CrowdStrike tenant, and enable CSPM Alerts ingestion. Repeat for additional tenants under the same Vanta domain.

- Adds threaded, @mention-enabled commenting on individual controls directly within a Vanta audit, replacing out-of-band email and Slack threads.
- Enables one-click export of the full controls table from within a Vanta audit for direct use in audit reports.
- Expands Vanta MCP connectivity to any MCP-capable tool (not just officially supported ones), with a warning banner when the redirect URL is outside Vanta-controlled origins.
- Adds 20 new privacy MCP tools covering data inventory and privacy assessments, enabling agentic automation of privacy program tasks.
- Introduces early-access pilot for AIUC-1, the new security standard for AI agents, available at no cost during the preview period.

+7 more

WAS THIS USEFUL? 👍 👎

◆ Integrated & IT Risk Management

LogicGate ⓘ

GRC Has Entered Its Agentic Era. Here's What That Means For Your Team. (2026-06-30)

2 RELEASES · 2026-06-11 → 2026-06-30 BLOG ↗ LATEST STABLE

LogicGate Spring 2026 introduces seven AI Workflow Agents, AI Governance module, expanded Spark AI, and enterprise-wide search across GRC use cases.

- Launches seven new AI Workflow Agents in early access spanning Third-Party Risk Management, Enterprise Risk Management, Business Continuity Management, and AI Governance use cases.
- New AI Governance module provides a unified view of AI risk: maps the full AI ecosystem, auto-calculates risk levels using NIST AI RMF categories, and surfaces business-impact indicators aligned to the EU AI Act and NIST frameworks.
- Adds Reporting Insights to Spark AI, enabling analysis of large data volumes within a single report with guided next-action recommendations.
- Introduces Automated Evidence Testing, which tests control evidence at the moment of collection to remove manual bottlenecks from the control lifecycle.
- Expands Config Newton (agentic GRC engineer) to work alongside in-house teams, enabling application deployment 50–75% faster plus bespoke reporting and end-user training assistance.

+3 more

▾ 1 more release in this issue · 2026-06-11 → 2026-06-30

The Agentic Era, Live: A Recap of Agility 2026 (2026-06-11) BLOG ↗ STABLE

LogicGate unveils Config Newton agentic GRC engineer and four new workflow agents for TPRM and AI governance.

- Introduces Config Newton, an agentic GRC engineer that interprets complex program requirements, navigates Risk Cloud, and autonomously builds complete GRC programs.
- New Third-Party Risk Management Agents automatically route vendors based on risk signals, complete formal assessments, and flag findings for human-led remediation.
- New AI Governance Agents triage incoming AI use cases, score them against your risk framework, and surface recommended mitigations for human review.
- All agent actions are fully logged and auditable, keeping practitioners in the decision loop while automating routine workflow progression.

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Claude Code ⓘ v2.1.207 NOTES ↗ CODE ↗

Claude Code is an agentic coding tool that lives in your terminal, understands your codebase, and helps you code faster by executing routine tasks, explaining complex code, and handling git workflows - all through natural language commands.

Auto mode goes GA on Bedrock/Vertex/Foundry, Opus 4.8 becomes the default, and plugin config scoping tightens.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.207 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.207
```

└──▷ USE IT

Opt out of auto mode on a Bedrock or Vertex deployment where you want to keep manual control over model selection.

```json
# In ~/.claude/settings.json
{
  "disableAutoMode": true
}
```

Migrate a per-repo auto mode override to the correct user-level settings file so it is still respected after this release.

```json
# Move autoMode from .claude/settings.local.json to ~/.claude/settings.json
{
  "autoMode": "auto"
}
```

Update a plugin hook that previously used shell-form `${user_config.*}` to the new exec-form with `$CLAUDE_PLUGIN_OPTION_<KEY>` to avoid the shell-injection rejection.

```json
# Before (now rejected):
# command: "my-hook --token ${user_config.api_token}"

# After — exec form with env var:
{
  "args": ["my-hook", "--token"],
  "env": { "TOKEN": "$CLAUDE_PLUGIN_OPTION_API_TOKEN" }
}
```

- Auto mode is now generally available on Bedrock, Vertex AI, and Foundry without the `CLAUDE_CODE_ENABLE_AUTO_MODE` opt-in flag; disable it via `disableAutoMode` in settings.
- Bedrock, Vertex, and Claude Platform on AWS now default to Claude Opus 4.8.
- Auto mode config is now read exclusively from `~/.claude/settings.json`; the repo-resident `.claude/settings.local.json` `autoMode` key is no longer honored (breaking change for teams using per-repo overrides).
- Plugin option values (`pluginConfigs`) are no longer read from project-level `.claude/settings.json`; only user-level, `--settings`, and managed settings are honored (breaking change for project-scoped plugin configs).
- Plugin hooks/monitors/MCP headersHelper: `${user_config.*}` interpolation in shell-form commands is now rejected; hooks must use exec form (`args` array) or `$CLAUDE_PLUGIN_OPTION_<KEY>` env vars instead (breaking change).

+2 more

└──▷ BREAKING ON UPGRADE

- ! Auto mode no longer reads `autoMode` from `.claude/settings.local.json` (repo-resident); use `~/.claude/settings.json` instead
- ! `${user_config.*}` in shell-form commands for plugin hooks/monitors/MCP headersHelper is now rejected; hooks must use exec form (`args` array) or `$CLAUDE_PLUGIN_OPTION_<KEY>`; monitors and headersHelper must read the value inside the script
- ! Plugin option values (`pluginConfigs`) are no longer read from project-level `.claude/settings.json`; only user, `--settings`, and managed settings are honored

WAS THIS USEFUL? 👍 👎

Pi ⓘ v0.80.6 7 RELEASES · 2026-06-18 → 2026-07-09 NOTES ↗ LATEST STABLE

AI agent toolkit: unified LLM API, agent loop, TUI, coding agent CLI

Pi v0.80.6 adds a `max` thinking level for GPT-5.6/Claude and input-token pricing tiers for long-context cost accounting.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.80.6 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.80.6
```

└──▷ TRY IT

Invoke the highest reasoning depth on a complex refactor task when using GPT-5.6 or a supported Claude model.

```
$ pi --thinking max 'Audit this codebase for insecure deserialization patterns and propose fixes'
```

- Adds `max` thinking level (above `xhigh`) for GPT-5.6 and adaptive Claude models, available via CLI, SDK, RPC, and model selection; custom themes can define `thinkingMax`.
- Adds request-wide input-token pricing tiers for accurate long-context cost accounting (e.g. GPT-5.4/5.5/5.6 rates), configurable in `models.json` and `modelOverrides`.
- Supports `~` (home directory) expansion in the `shellPath` setting.

▾ 6 more releases in this issue · 2026-06-18 → 2026-07-09

v0.80.3 NOTES ↗ STABLE

Pi v0.80.3 adds Claude Sonnet 5, Azure Foundry endpoints, new RPC session APIs, and configurable editor/padding settings.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.80.3 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.80.3
```

└──▷ USE IT

Override the Ctrl+G external editor to use a specific binary (e.g. vim) instead of the environment default.

```json
// In settings.json
{ "externalEditor": "vim" }
```

Tighten or expand terminal padding for assistant and thinking output to improve readability in narrow or wide terminals.

```json
// In settings.json
{ "outputPad": 4 }
```

- Adds Anthropic Claude Sonnet 5 support via Anthropic-compatible and Bedrock provider catalogs, with adaptive thinking enabled.
- Supports modern Microsoft Azure Foundry endpoint URLs for the Azure OpenAI Responses provider.
- New `get_entries` and `get_tree` RPC commands let clients inspect session entries and tree snapshots programmatically.
- New `./rpc-entry` package export enables launching Pi directly in RPC mode.
- New `session_info_changed` extension event lets extensions observe session name changes.

+4 more

└──▷ BREAKING ON UPGRADE

! The default OpenAI model is changed to `gpt-5.5`.

v0.80.0 NOTES ↗ STABLE

Pi v0.80.0 adds Ctrl+J newline keybinding and migrates pi-ai's global API to a new compat entrypoint.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.80.0 https://github.com/earendil-
works/pi.git
# already have the repo? check out this version:
$ git checkout v0.80.0
```

› Adds `Ctrl+J` as a default newline keybinding alongside `Shift+Enter`.

› Moves pi-ai's legacy global API (`stream` / `complete` / `completeSimple`, `getModel` / `getModels` / `getProviders`, `registerApiProvider`, `getEnvApiKey`, etc.) from the `@earendil-works/pi-ai` root to `@earendil-works/pi-ai/compat`; extension sources typechecking against pi-ai's published types should update imports accordingly or migrate to the new createModels() `/provider-factory` API.

› Removes the `@earendil-works/pi-ai/base` and `@earendil-works/pi-agent-core/base` selective-provider entrypoints; use the root packages with explicit `Models` provider factories instead.

└──▷ **BREAKING ON UPGRADE**

! The `@earendil-works/pi-ai/base` and `@earendil-works/pi-agent-core/base` entrypoints have been removed; use the root packages with explicit `Models` provider factories instead.

! The global API (`stream` / `complete` / `completeSimple`, `getModel` / `getModels` / `getProviders`, `registerApiProvider`, `getEnvApiKey`, etc.) has been moved off the `@earendil-works/pi-ai` root entrypoint to `@earendil-works/pi-ai/compat`; extension sources that typecheck against pi-ai's published types must switch those imports to `@earendil-works/pi-ai/compat` or migrate to the new createModels() `/provider-factory` API.

v0.79.10 NOTES ↗ STABLE

Extension compaction events gain reason/willRetry context; pi update now pins the exact checked version.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.79.10 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.79.10
```

└──▷ **USE IT**

React differently in a custom summarization extension depending on whether compaction was triggered manually, by a threshold, or as an overflow retry.

```javascript
// In your extension handler:
extension.on('session_before_compact', ({ reason, willRetry }) => {
  if (reason === 'overflow' && willRetry) {
    // overflow retry: use a lighter summary to reduce token cost
  } else if (reason === 'manual') {
    // user-initiated /compact: run full archival summary
  }
});
```

- Adds `reason` and `willRetry` metadata to `session_before_compact` and `session_compact` extension events, enabling extensions to distinguish manual `/compact`, threshold auto-compaction, and overflow retry flows.
- Updates `pi update` to install the exact version returned by the Pi update check and surface the changelog URL in update notices, making upgrade behavior predictable.

v0.79.9 NOTES ↗ STABLE

Pi v0.79.9 adds chat-template thinking support for vLLM/Hugging Face providers like DeepSeek and improves GLM-5.2 routing.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.79.9 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.79.9
```

- Adds chat-template thinking support: OpenAI-compatible custom providers can now map Pi thinking levels into `chat_template_kwargs`, enabling vLLM/Hugging Face models such as DeepSeek to use provider-native thinking controls.
- Enables GLM-5.2 `xhigh` reasoning on OpenRouter and corrects Fireworks routing to use the OpenAI-compatible Chat Completions endpoint with `reasoning_effort` support.

v0.79.8 NOTES ↗ STABLE

Pi v0.79.8 adds Mistral prompt caching, OpenRouter Fusion alias, and post-compaction token estimates.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.79.8 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.79.8
```

- Adds Mistral prompt caching using the Pi session ID as the cache key, with cached-token usage and cost accounting surfaced per session.
- Adds `openrouter/fusion` as a built-in OpenRouter model alias for direct use as a provider target.
- Adds estimated post-compaction token counts to compact results and compaction events, letting clients display approximate context reduction.
- Adds `@earendil-works/pi-ai/base` and `@earendil-works/pi-agent-core/base` entry points for SDK users who need selective provider registration to trim bundle size.

v0.79.7 NOTES ↗ STABLE

Pi v0.79.7 adds automatic light/dark theme switching, scoped update control, and new extension API exports.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.79.7 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.79.7
```

└──▷ TRY IT

Update pi and all extensions in one shot when you want everything on the latest version.

```
$ pi update --all
```

- Adds automatic theme mode in `/settings` to assign separate light and dark themes that follow terminal color-scheme changes.
- Changes `pi update` to update only pi by default; new `pi update --all` updates pi and all extensions together.
- Exports `generateDiffString`, `generateUnifiedPatch`, and `EditDiffResult` from the public API for extensions that produce edit-style diffs.

› Enables inline image rendering in Warp terminals via automatic Kitty graphics protocol detection.

└──▷ BREAKING ON UPGRADE

! The `pi update` command now updates only pi itself; the previous behaviour of updating pi and packages together now requires `pi update --all`.

WAS THIS USEFUL? 👍 👎

Cline ⓘ v4.0.8 NOTES ↗ CODE ↗

Autonomous coding agent as an SDK, IDE extension, or CLI assistant.

GCP Vertex provider gains new Claude models and a free-form model ID entry field.

└──▷ GET THIS VERSION

```
$ git clone --branch v4.0.8 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout v4.0.8
```

› Adds new Claude model IDs to the GCP Vertex provider, including claude-sonnet-5, claude-opus-4-x variants, claude-haiku-4-5, and claude-fable-5.

› Enables free-form model ID entry in the Vertex provider's model dropdown, letting practitioners use any Vertex-hosted model without waiting for an extension release.

WAS THIS USEFUL? 👍 👎

OpenHands ⓘ cloud-1.46.0 NOTES ↗

OpenHands: AI-Driven Development

OpenHands 1.46 adds configurable BYOR key alias patterns and enriched final archive manifests.

└──▷ GET THIS VERSION

```
$ git clone --branch cloud-1.46.0
https://github.com/OpenHands/OpenHands.git
# already have the repo? check out this version:
$ git checkout cloud-1.46.0
```

- Supports configurable Bring-Your-Own-Router (BYOR) key alias patterns for enterprise deployments.
- Enriches final archive manifests with additional metadata and removes redundant initial snapshots.

WAS THIS USEFUL? 👍 👎

Cursor ⓘ Side Chats and Conversation Search NOTES ↗

Cursor is an AI-powered code editor that helps developers write, edit, and debug code faster using integrated large language model assistance.

Cursor adds side chats, agent transcript search, new cloud agent hooks, and redesigned project/repo pickers.

.

└──▷ HOW TO FIND IT

Spin up a side chat to sanity-check a design decision while the main agent keeps running — without losing your place.

> 📍 In the chat panel, type `/side` or `/btw` to open a new side chat that already has context from your main conversation.

Find a specific past agent conversation by searching full transcripts, not just names or PR numbers.

> 📍 In the Agents Window, press Cmd+K and type keywords from the transcript content to locate the conversation.

Build a self-correcting agent loop by intercepting responses and controlling subagent behavior via new cloud agent hooks.

> 📍 In your cloud agent hook configuration, register handlers for beforeSubmitPrompt, afterAgentResponse, afterAgentThought, stop, and subagentStart to observe reasoning and inject corrections. See supported hooks in the Cursor docs.

- New Side Chats: open parallel agent conversations via `/side`, `/btw`, or the plus button without interrupting the main agent thread — each is a durable, full agent conversation that can be revisited and @`-mentioned`.
- Adds agent transcript search in the Agents Window via Cmd+K (command palette), with a local search index that scales to thousands of conversations.
- Adds in-conversation search with Cmd+F, match counter, and jump-between-matches for long agent transcripts.
- New cloud agent hooks (`beforeSubmitPrompt`, `afterAgentResponse`, `afterAgentThought`, `stop`, `subagentStart`, and more) enable observing and controlling prompts, responses, reasoning, subagents, compaction, and turn completion.
- Redesigned project and repo pickers support creating a project and connecting GitHub, GitLab, or Azure DevOps without leaving the picker.

+4 more

WAS THIS USEFUL? 👍 👎

Windsurf ⓘ snapshot-20260711 NOTES ↗

Windsurf is an AI-powered code editor that helps developers write, edit, and navigate code faster using intelligent autocomplete and agentic AI assistance.

└──▷ **USE IT**

Exclude a sensitive command (e.g., a secret-scanning script) from the sandbox so it runs with full environment access, enforced for the whole team.

json

```
{
  "sandbox": {
    "excluded": {
      "deny": ["run-secret-scan.sh"],
      "allow": ["git", "make test"]
    }
  }
}
```

Check how many ACUs your current Devin session has consumed without leaving the chat.

```
$ /usage
```

Suppress Devin attribution lines in commit messages made by the local agent — useful when commits must conform to org policy.

json

```
{
  "attribution": false
}
```

- Skill permissions: frontmatter definitions now apply to auto-approvals.
- Enterprise login policies are now enforced in the CLI.
- Adds server-level MCP tool permission options: approve all tools on a server for the current session, or permanently.
- Introduces Devin for Terminal — a CLI agent running locally in Rust with multi-model support and seamless hand-off to Devin Cloud.
- Integrates Devin Cloud agent directly inside Windsurf, available with every self-serve plan, allowing one-click delegation to a cloud VM.

WAS THIS USEFUL? 👍 👎

AGENT

◆ AI Agent Frameworks

LangGraph ⓘ cli==0.4.31 NOTES ↗

Build resilient agents.

LangGraph CLI now supports prebuild images for langgraph deploy.

└──▷ GET THIS VERSION

```
$ git clone --branch cli==0.4.31 https://github.com/langchain-ai/langgraph.git
# already have the repo? check out this version:
$ git checkout cli==0.4.31
```

› Supports prebuild images when running `langgraph deploy`, enabling faster deployments using pre-built Docker images.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 11, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe