THE CYBER TOOLCHAIN

NO. 140

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED NOVEMBER 15, 2026 · EVERY DAY

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

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 90 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 23 tools

▾ // THE BRIEF

HIDE SAME ISSUE, SAME PROMPT, TWO WRITERS: GPT-5.5 | Opus 5

What stands out across today's releases, grouped by what it lets you do. Every tool named links to its entry below.

Three unrelated things stand out today: MobSF can now inspect hybrid mobile apps and Hermes bytecode, Semgrep makes dependency paths

vim ? help

and AI-assisted triage cheaper to use, and Secretlint removes setup friction while making secret scans much faster.

PROTECT

Scan more mobile app surfaces before release

MobSF added JavaScript/TypeScript and hybrid app analysis, Hermes bytecode decompilation, Flutter scanning, expanded iOS checks, and in-process Windows APPX/MSIX static analysis. That closes a common blind spot where mobile review stopped at native code or required separate tooling for packaged web and hybrid content.

MobSF

PROTECT

Trace vulnerable dependencies to the code path that pulls them in

Semgrep added Supply Chain dependency-path tracing, while Cloudsmith enriched vulnerability records with EPSS exploitability scores. Teams get better triage inputs: not just that a package is vulnerable, but whether it is likely to be exploited and how it entered the application graph.

Semgrep · Cloudsmith

PROTECT

Make secret and web findings easier to run and verify

Secretlint now bundles recommended rules without requiring a config file, adds `--profile`, and reports 7x-24x faster scans. xalgorix now keeps scans to the authorized host and emits ready-to-run curl commands for every HTTP/HTTPS finding, reducing the back-and-forth needed to reproduce and validate results.

Secretlint · xalgorix

PROTECT

Put guardrails around AI and egress paths

Varonis added gateways and browser-level controls for AI agent and LLM usage, giving teams a policy point for risky AI interactions instead of relying on user guidance alone. minimal added a Box Egress Proxy with client-key limits and a named-secret store, narrowing how outbound access and stored secrets are handled.

Varonis

Does **GPT-5.5** read better? 👍 👎

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

xalgorix

Feedback ⓘ v4.6.192 NOTES ↗ RANK

Xalgorix autonomous AI pentesting agents — real-time reconnaissance, vulnerability detection, and exploitation orchestration. Go + TypeScript.

> Xalgorix tightened scan scope to the authorized host and made every HTTP/HTTPS finding reproducible with a ready-to-run curl command.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **Replayable curl command in findings** IMPROVED 77

Every HTTP/HTTPS finding now includes a copy-pasteable `curl` command in its proof of concept, built from the finding's reported method and endpoint when the agent did not already produce one — literal `../` path-traversal segments, URL encoding, and shell-quoting are preserved so the request replays exactly.

— Concrete, runnable output with preserved encoding details named v4.6.190

THINNER COVERAGE BELOW

02 **Third-party domain scanning restriction** IMPROVED 53

Single-host scans now skip third-party domains — CDNs, partner backends, and external APIs discovered in the target's pages, redirects, or JavaScript — noting them but not scanning them, keeping requests within the authorized host.

— Explains mechanism and scope but no config surface named v4.6.192

WAS THIS USEFUL? 👍 👎

RedAmon

Feedback ⓘ v7.8.0 NOTES ↗ RANK

RedAmon is an open-source, self-hosted AI penetration testing. RedAmon maps your attack surface into a graph, exploits it with human approval gates and opens PRs that fix it.

> RedAmon's v7.8.0 release introduces multi-user RBAC with granular on/off switches, a new IAM console, project sharing with ownership transfer, hostname-aware scanning modes, and a 98-permission enforcement registry — alongside several breaking security changes including plaintext secret storage, non-root MCP execution, and restricted saved graph queries.

└──▷ **WHAT SHIPPED · 15 FEATURES** most completely described first ? what's the number?

01 **Granular RBAC subsystem switches** BREAKING 95

Control the five RBAC subsystems independently with `RBAC_IDENTITY_ENABLED`, `RBAC_PERMISSIONS_ENABLED`, `RBAC_SHARING_ENABLED`, `RBAC_SHARING_WRITE_ENABLED`, and `RBAC_GOVERNANCE_ENABLED` in `.env` — all default on, so the update enables them unless `.env` already sets them, changing access-control behaviour on existing installs; set any to `false` before updating to keep it off. Downgrading to 7.7.2 drops every table and column added since, along with their data — run `docker compose exec webapp node scripts/rbac-upgrade-preview.mjs --downgrade` and back up the database before attempting it.

Keep RBAC sharing disabled on an existing shared server while you review legacy user grants before the rollout.

```ini
RBAC_IDENTITY_ENABLED=true
RBAC_PERMISSIONS_ENABLED=true
RBAC_SHARING_ENABLED=false
RBAC_SHARING_WRITE_ENABLED=false
RBAC_GOVERNANCE_ENABLED=false
```

— Names all five env vars and the downgrade command v7.8.0

02 **Hostname scanning modes for IP-mode projects** NEW 80

IP-mode projects now add a hostname scanning mode selector with four options: IP only (default), Record hostnames, Record + scan matching, and Record + scan all — controllable via MCP with `create_project` and `update_project_scope`.

— Names all four modes and the two MCP calls v7.8.0

03 **Metasploit project console leasing** BREAKING 75

Metasploit now serves one project at a time; a project releases its console 10 minutes after the last command, adjustable via `MSF_PROJECT_LEASE_IDLE_S` in `.env` (default: 10 minutes).

— Explains mechanism and names the config key v7.8.0

04 **Project sharing and ownership transfer** NEW 75

Adds project sharing at Viewer (Read) and Analyst (Read + Raw data and files) levels with an optional end date, a note, and a Shared with me view on the Projects page; ownership transfer at the Read + Write share level moves the graph, settings, and history atomically after both parties confirm with their password; admins holding `projects:oversee` (Full admin or Security auditor role) can open any project read-only once sharing is active, with each read audited and shown to the owner.

— Rich mechanism but no exact command or endpoint v7.8.0

05 **Named permission registry and enforcement** NEW 75

RedAmon adds a registry of 98 named permissions enforced by a single policy on every route, with MCP tokens capped to their owner's permissions; agent phase approvals now require `agent:approve_phase` or `agent:approve_dangerous` permissions.

— Names specific permission strings and scope v7.8.0

06 **Root assignment via CLI or env var** NEW 70

Set Root on the command line with `./redamon.sh set-root <email>` or via `ADMIN_EMAIL` in a deploy environment.

Promote a specific admin account to Root from the terminal after a multi-admin upgrade.

📍 ./redamon.sh set-root admin@example.com

— Runnable command and env var named v7.8.0

07 **IAM console at /admin** BREAKING 70

The header Users page is replaced by a multi-user IAM console at `/admin`, with sections for users, permission sets, admin profiles, every project and share, quotas, per-plugin allowlists, instance LLM providers, sharing policy, audit retention, and the audit log.

— Names every console section but only a UI path v7.8.0

08 **Audit event forwarding to stdout** NEW 65

Print every audit event as a JSON line for a log pipeline by setting `AUDIT_FORWARD=stdout` in `.env`.

Forward all audit events to a SIEM or log pipeline by printing each as a JSON line to stdout.

```ini
AUDIT_FORWARD=stdout
```

— Exact config key and value given v7.8.0

09 **stdio MCP servers run as non-root uid** BREAKING 65

stdio MCP servers now run as uid 10001 instead of root; tools installed under `/root` must be moved to a system-wide path or their directory `chown`ed to 10001.

— Gives exact uid and remediation action v7.8.0

10 **Admin session security hardening** IMPROVED 60

Admin sessions are now limited to 12 hours with a 60-minute idle timeout and support sign-out of individual device sessions; sign-in enforces a 12-character minimum password floor and no longer reveals whether an account exists.

— Concrete limits but no command or config key v7.8.0

THINNER COVERAGE BELOW

11 **Saved graph query restrictions** BREAKING 55

Saved graph views that use `shortestPath`, `apoc` calls, or non-standard characters (such as a non-breaking space) are now refused with HTTP 400.

— Names exact refused functions and status code v7.8.0

12 **Secrets now stored in clear text** BREAKING 50

Neo4j database, graph snapshots, project exports, and the recon JSON now store found secrets in clear text; database access and exported files must be treated as credential material.

— Clear warning but no mitigation step given v7.8.0

13 **ZAP Ajax Spider memory allocation raised** BREAKING 35

`BROKER_TOOL_MEM_BYTES` was raised to `3g` in 7.6.2; a lower value in `.env` starves the ZAP Ajax Spider.

— Thin historical note, single value cited v7.8.0

14 **Per-project tool image settings removed** DEPRECATED 30

The 17 per-project tool image settings were removed in 7.7.0; tool images are now fixed.

— States removal only, no replacement detail v7.8.0

15 **Agent-in-the-loop and MCP server forced on** BREAKING

30

7.6.0 enables `AGENT_IN_THE_LOOP_ENABLED` and `MCP_SERVER_ENABLED` once, even where `MCP_SERVER_ENABLED=false` was previously set.

— Names flags but no mitigation or mechanism v7.8.0

└──▷ **BREAKING ON UPGRADE**

! The five RBAC switches (`RBAC_IDENTITY_ENABLED`, `RBAC_PERMISSIONS_ENABLED`, `RBAC_SHARING_ENABLED`, `RBAC_SHARING_WRITE_ENABLED`, `RBAC_GOVERNANCE_ENABLED`) are on by default; the update enables them unless `.env` already sets them, changing access-control behaviour on existing installs.

! The header `Users` page is replaced by `IAM` at `/admin`.

! stdio MCP servers now run as uid 10001 instead of root; tools installed under `/root` must be moved to a system-wide path or their directory `chown`ed to 10001.

! Metasploit now serves one project at a time; a project releases its console 10 minutes after the last command (adjustable via `MSF_PROJECT_LEASE_IDLE_S`).

! Neo4j database, graph snapshots, project exports, and the recon JSON now store found secrets in clear text; database access and exported files must be treated as credential material.

! Saved graph views that use `shortestPath`, `apoc` calls, or non-standard characters (such as a non-breaking space) are now refused with HTTP 400.

! Downgrading to 7.7.2 drops every table and column added since, along with their data; run `docker compose exec webapp node scripts/rbac-upgrade-preview.mjs --downgrade` and back up the database before attempting it.

! `BROKER_TOOL_MEM_BYTES` was raised to `3g` in 7.6.2; a lower value in `.env` starves the ZAP Ajax Spider.

! The 17 per-project tool image settings were removed in 7.7.0; tool images are now fixed.

! 7.6.0 enables `AGENT_IN_THE_LOOP_ENABLED` and `MCP_SERVER_ENABLED` once, even where `MCP_SERVER_ENABLED=false` was previously set.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Code Security

GitHub

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗

GitHub is a web-based platform for version control and collaborative software development using Git repositories.

GitHub adds an AI Scan REST API, three new Copilot models, Dependabot pause on inactive repos, personal-account issue types, and alert direct links.

Manage AI Scan for repositories via the REST API, enabling automated governance of AI-generated code scanning at scale.

NEW INTEGRATION Gemini 4 Hydrogen is now available as a model option in GitHub Copilot.

Gemini 4 Carbon is now available as a model option in GitHub Copilot.

Claude Fable 5.2 is now available as a model option in GitHub Copilot.

Issue types and fields are now available for personal account projects, bringing structured issue metadata to individual users.

+3 more

NEW DETECTION Secret scanning detects secrets in GitHub Actions workflow logs

NEW DETECTION Secret scanning detects Cloudflare service tokens

└──▷ BREAKING ON UPGRADE

! Actions for ARM32 Linux and Windows are being retired.

! Selected GitHub Copilot models are scheduled for deprecation in December.

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗ RANK

Veracode is a cloud-based application security platform that scans code for vulnerabilities using static, dynamic, and software composition analysis testing methods.

> Veracode rolled out its modernized application page UI to all FedRAMP customers, adding engine version pinning and in-page SCA scanning while retiring the legacy UI for that region.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 **Static analysis engine version pinning** NEW 73

Customers can pin static analysis engine versions at the application profile level, a capability not available in the legacy UI. In the Veracode Platform, open the application profile, go to application settings, locate Static analysis engine version pinning, and select the engine version to lock so scan results stay comparable across builds.

Lock a project to a specific static analysis engine version so scan results stay comparable across builds — reach this setting inside the application profile after signing in to the new UI.

> 📍 In the Veracode Platform, open the application profile › navigate to the application settings › locate Static analysis engine version pinning and select the engine version to lock.

— Exact navigation path given but no scope/limit details changelog-20261115-59743bc7

02 **Upload and Scan SCA from application profile** NEW 65

Users can run Upload and Scan SCA scans directly from individual application profiles in the new UI, a capability not available in the legacy UI. In the Veracode Platform, open the application profile and select Upload and Scan SCA to initiate an SCA scan scoped to that application.

Kick off an SCA scan without leaving the application profile page — useful when you want SCA results alongside static findings for the same app.

> 📍 In the Veracode Platform, open the application profile › select Upload and Scan SCA to initiate an SCA scan scoped to that individual application profile.

— Clear UI steps but no detail on scan mechanics changelog-20261115-59743bc7

THINNER COVERAGE BELOW

03 **Modernized UI enabled for FedRAMP, legacy retired** BREAKING

Veracode's modernized application page UI is now enabled for all FedRAMP customers, and the legacy application page UI has been retired for that region, making it no longer available to them.

— States rollout and removal but no migration guidance changelog-20261115-59743bc7

└──▷ **BREAKING ON UPGRADE**

! The legacy application page UI has been retired for FedRAMP customers and is no longer available to them.

WAS THIS USEFUL? 👍 👎

Semgrep

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗ RANK

Get started with Semgrep to help you catch, flag, and fix real vulnerabilities before they ship.

> Semgrep shipped a hosted MCP server for AppSec Platform, an observe-only mode for Guardian, and bring-your-own AI provider keys for Agentic Workflows, alongside Supply Chain dependency-path tracing, expanded language parsing, and a tenfold cut in autotriage credit cost.

└──▷ **WHAT SHIPPED · 10 FEATURES** most completely described first ? what's the number?

01 MCP server scanning and hosted AppSec Platform server NEW

95

`semgrep_scan` in the MCP server can now scan files outside the client workspace via `SEMGREP_MCP_ALLOW_SCAN_OUTSIDE_WORKSPACE=true`. A new hosted Model Context Protocol (MCP) server for AppSec Platform (public beta) is reachable from Claude Code, Codex, Cursor, VS Code, or any MCP client via `semgrep mcp` to search and triage findings, run scans, and manage policies from an editor or terminal.

— Names exact env var, command, and supported clients. changelog-20261115-83ba9aa3

02 Supply Chain dependency path, exit codes, and matching ranges

IMPROVED

93

Supply Chain now shows the dependency path for transitive findings in Go projects when dependency paths are turned on and local builds are allowed with `--allow-local-builds`. Running `semgrep ci --no-suppress-errors` with `--allow-local-builds` now exits with code `2` when dependency resolution fails for a subproject, listing affected dependency sources while still reporting findings from other subprojects. Incident cards now show how many projects have matching ranges — projects whose file declares an affected Python package with a version range or without a version — in a new `Potentially matching: declared in a version range` section listing each project, branch, file, and declared version.

Show transitive Go dependency paths for a Supply Chain scan when running local builds, so each vulnerable transitive package is traceable to its direct dependency.

```
$ semgrep ci --allow-local-builds --no-suppress-errors
```

— Names exact flags, exit code, and new UI section. changelog-20261115-83ba9aa3

03 Guardian observe-only mode and Copilot CLI beta NEW

80

Guardian gains an observe-only mode, enabled via `SEMGREP_GUARDIAN_OBSERVE_ONLY=1`, letting Guardian scan as usual while hiding results from developers and coding agents so teams can audit findings before rollout. Guardian for GitHub Copilot CLI also enters public beta on macOS and Linux.

Roll out Guardian to a team in observe-only mode first to audit what it finds without surfacing alerts to developers.

```
$ export SEMGREP_GUARDIAN_OBSERVE_ONLY=1
```

— Names exact env var and rollout mechanism. changelog-20261115-83ba9aa3

04 **Agentic Workflows AI provider keys and issue notes** NEW

78

Agentic Workflows now accept bring-your-own API keys for OpenAI, Anthropic, Google Gemini, xAI, and Microsoft Foundry, used for all model requests and AI-powered detection instead of Semgrep-managed OpenAI or Amazon Bedrock, with Microsoft Foundry (formerly Azure OpenAI) getting its own card in AI provider settings accepting a resource endpoint, an API key, and one or more deployments each with its model; and notes can now be added to Agentic Workflows issues via a New note button at the top of an issue's activity.

— Names all five providers and Foundry's config fields. Names exact UI button location. changelog-20261115-83ba9aa3

05 **Intel Mac CLI binaries discontinued** BREAKING

70

The Semgrep CLI no longer ships binaries for Intel Macs; version 1.182 is the last release that supports them. Intel Mac users should upgrade to the `semgrep/semgrep` Docker image or move to Apple silicon with a native arm64 Python.

— Names exact last supported version and migration paths. changelog-20261115-83ba9aa3

06 **Ignore rate replaces false positive rate metric** IMPROVED

65

The False positive rate column in the rules table is now Ignore rate, counting findings triaged as ignored for any reason plus findings ignored with a `nosemgrep` comment, with per-triage-reason counts visible on hover.

— Names exact column rename and counting logic. changelog-20261115-83ba9aa3

07 **Open-source dependency licenses link in CLI help** NEW

60

A link to Semgrep's open-source dependency licenses now appears in the `--help` output of most `semgrep` commands under a new `THIRD-PARTY LICENSES` section

pointing to `semgrep.dev/cli-credits`.

— Exact section name and URL but minor scope. changelog-20261115-83ba9aa3

THINNER COVERAGE BELOW

08 **Parser support for Bash, Clojure, and Swift 5.9 syntax**

IMPROVED 58

Semgrep Code now parses newer Bash arithmetic expressions such as $(($X * 2)), Clojure files using reader-evaluated metadata (^#=(...)) or the legacy `#^` prefix, and Swift 5.9 syntax including macros, parameter packs, and `if` / `switch` expressions.

— Names exact syntax forms parsed, no usage command. changelog-20261115-83ba9aa3

09 **Autotriage credit cost reduced tenfold** IMPROVED 50

Autotriage cost drops from 1 AI credit per finding to 0.1 credits (10 triages per credit) starting October 31, 2026, for paid plans, trials, and the free plan.

— Precise numbers and date, no action needed. changelog-20261115-83ba9aa3

10 **Lower minimum seat count for self-service plans** IMPROVED 40

Minimum seat count for new self-service purchases of Semgrep Code, Semgrep Supply Chain, or Semgrep Secrets drops from 10 to 3.

— Specific numbers, no further mechanism. changelog-20261115-83ba9aa3

└──▷ **BREAKING ON UPGRADE**

! The Semgrep CLI no longer ships binaries for Intel Macs; version 1.182 is the last release that supports them. Upgrade Intel Mac users to the `semgrep/semgrep` Docker image or move to Apple silicon with a native arm64 Python.

WAS THIS USEFUL?  

psalm-plugin-laravel

Feedback ⓘ v4.20.0 NOTES ↗ RANK

Psalm-plugin-laravel is a security-focused Laravel static analyser

> Psalm-plugin-laravel v4.20.0 improves migration analysis for morph columns and adds support for `@mixin \Eloquent` models, while bumping its Psalm dependency requirements.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 **UUID/ULID typing for morph columns** IMPROVED 75

The plugin now honors Schema::morphUsingUuids() and Schema::morphUsingUlids() for morphs() and nullableMorphs() columns in migration analysis: the `*_id` column is now typed as `string` instead of `int` when these UUID/ULID morph modes are used.

– Names exact methods and before/after type change v4.20.0

02 **@mixin \Eloquent model support** NEW 62

Models annotated with `@mixin \Eloquent` (as written by laravel-ide-helper's `ide-helper:models --write`) or another custom `@mixin` are now supported, along with inherited `#[UseEloquentBuilder]`, so that builder calls on these models resolve correctly.

– Names annotation and source command but no example v4.20.0

03 **Raised Psalm dependency requirements** BREAKING 60

This release requires `vimeo/psalm` `^7.5.0` (previously `^7.3.1`) and `psalm/psalm-plugin-api` `^0.4.3`.

– Exact version constraints given, no migration notes v4.20.0

└──▷ **BREAKING ON UPGRADE**

! Requires `vimeo/psalm` `^7.5.0` (previously `^7.3.1`) and `psalm/psalm-plugin-api` `^0.4.3`.

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

Cloudsmith

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗

RANK

Cloudsmith is a fully-managed artifact management, software supply chain security, and software distribution platform.

> Cloudsmith added Hugging Face Tree API support for CLI-based model downloads, enriched vulnerability records with EPSS exploitability scores, and made several CLI and logging quality-of-life improvements.

└──▷ **WHAT SHIPPED · 3 FEATURES** most completely described first ? what's the number?

01 **Hugging Face Tree API support** NEW 67

Cloudsmith now serves Hugging Face's Tree API so `hf download` and `snapshot_download` work through Cloudsmith on `huggingface_hub` 1.22 and later.

— Names exact API, commands and version requirement but no further mechanism.

changelog-20261115-3ab84ab4

THINNER COVERAGE BELOW

02 **EPSS scores on vulnerability records** NEW 48

Vulnerability records now show EPSS scores so you can prioritize High and Critical findings by likelihood of exploitation, not just severity.

— Clear benefit named but no UI path or API detail given. changelog-20261115-3ab84ab4

03 **Request-chain visibility in client log exports** IMPROVED 40

Client log exports now include format-specific metadata requests alongside downloads, giving visibility into the full request chain behind a download.

— Describes the change but no field names or export format specifics.

changelog-20261115-3ab84ab4

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

Secretlint

Feedback ⓘ v14.0.0 NOTES ↗ RANK

Secretlint is a pluggable linting tool to prevent committing credential.

> Secretlint v14 eliminates the need for a config file by bundling the recommended rules directly into the package, adds a `--profile` flag for performance diagnostics, and claims 7x-24x faster scans alongside a set of breaking changes to its ignore-file handling and rule plugin API.

└──▷ **WHAT SHIPPED · 8 FEATURES** most completely described first ? what's the number?

01 Breaking changes to rule plugin API

BREAKING 85

Lint results and `--format json` output no longer contain `sourceContent`; formatters now receive getSource(filePath) instead. `configFilePath` returned by loadConfig() and loadConfigDescriptor() is now `string | undefined` instead of always a string. The `enableIDScanRule` option of the aws rule must now be a boolean (`true`), not a string (`"true"`). Files are linted in any order, so a rule must not keep state between files. `"all"` is removed from `SecretLintRuleContentType`, and `create` is now optional in `SecretLintRuleCreator`.

— Enumerates every API surface change with before/after types v14.0.0

02 Ignore-file handling: `--no-gitignore` and `--secretlintignore`

80

BREAKING

`--no-gitignore` opts out of `.gitignore` cascading so files Git would normally exclude can be scanned. `--secretlintignore <path>` reads an extra ignore list as a path from the current directory, combined with `.secretlintignore` rather than replacing it. `.gitignore` files are now part of the combined ignore set, and a `!` re-include rule only applies within the same ignore-file kind.

Scan build artifacts or other files excluded by `.gitignore` — useful for verifying generated output before release.

```
$ secretlint --no-gitignore "dist/**/*"
```

— Names both flags and the combined-ignore mechanism with a runnable example v14.0.0

03 Built-in rules bundled into `@secretlint/core`

BREAKING

80

Installing only `secretlint` now provides all official rules bundled inside `@secretlint/core` — separate rule packages (`@secretlint/secretlint-rule-preset-recommend` , `@secretlint/secretlint-rule-aws` , and others) are no longer published and installed copies are ignored, with rule ids resolving from the bundle. Code that imported a rule from `@secretlint/secretlint-rule-*` must now import it from `@secretlint/core/builtin/rules/<name>` .

— Names old and new package/import paths precisely v14.0.0

04 **`--profile` performance summary flag** NEW

70

Profile scan performance by phase, rule, pattern, and file using `--profile` ; this now prints a performance summary instead of lint results.

Identify where scan time is going across phases, rules, patterns, and files after optimizing a large repo.

```
$ secretlint --profile "**/*"
```

— Named flag with runnable example and clear output change v14.0.0

05 **`--secretlintrc` single-file resolution** BREAKING

65

`--secretlintrc <path>` now resolves exactly one config file from the current directory; parent-directory search and automatic extension appending are no longer performed.

— Exact before/after behavior for a named flag, no example given v14.0.0

06 **Zero-config operation with recommended rules** BREAKING

60

Running Secretlint with no configuration file now applies the recommended rules automatically, instead of exiting with status 2 as before.

Scan an entire repo with no config file — recommended rules run automatically without any setup.

```
$ npx secretlint "**/*"
```

— Clear before/after but no mechanism beyond rule auto-selection v14.0.0

THINNER COVERAGE BELOW

07 **Declarative rule patterns with `patterns` and `keywords`** NEW

55

Write declarative rule patterns using `patterns` with `keywords` so Secretlint skips files containing no matching keyword, keeping custom rule scans fast.

— Names the config keys but no runnable example v14.0.0

08 Faster scanning via keyword pre-filtering IMPROVED

55

Large repositories scan 7x to 24x faster through keyword pre-filtering and worker-thread file reading, without native modules or WebAssembly.

— Explains mechanism and gives a figure but no actionable command v14.0.0

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! Running with no configuration file now applies the recommended rules instead of exiting with status 2.

! `--secretlintrc <path>` now resolves exactly one file from the current directory and no longer searches parent directories or appends a file extension.

! `--secretlintignore <path>` is now a path from the current directory and is read in addition to `.secretlintignore` rather than replacing it.

! `.gitignore` files are now part of the combined ignore set; a `!` rule only re-includes files within the same ignore-file kind.

! The `enableIDScanRule` option of the aws rule must now be a boolean (`true`), not a string (`"true"`).

! `--profile` now prints a performance summary instead of lint results.

! Results and `--format json` output no longer contain `sourceContent` ; formatters now receive getSource(filePath) instead.

! `configFilePath` returned by loadConfig() and loadConfigDescriptor() is now `string | undefined` instead of always a string.

! Files are linted in any order; a rule must not keep state between files.

! `"all"` is removed from `SecretLintRuleContentType` , and `create` is now optional in `SecretLintRuleCreator` .

! Code that imported a rule from `@secretlint/secretlint-rule-*` must now import it from `@secretlint/core/builtin/rules/<name>` .

! Official rule packages (`@secretlint/secretlint-rule-preset-recommend` , `@secretlint/secretlint-rule-aws` , and others) are no longer published from v14; installed copies are ignored and rule ids resolve from the bundle inside `secretlint` .

WAS THIS USEFUL? 👍 👎

◆ Mobile App Security

MobSF

Feedback ⓘ v4.6.6 NOTES ↗ RANK

MobSF is an automated mobile application pen-testing, malware analysis and security assessment framework for Android, iOS and Windows apps, with static and dynamic analysis.

> MobSF adds JavaScript/TypeScript and hybrid mobile app analysis with Hermes bytecode decompilation, brings Windows APPX/MSIX static analysis fully in-process, and expands iOS entitlements, binary and SBOM-adjacent checks, alongside new malware-domain lookups, Flutter scanning and a rate limiter for threat-database updates.

└──▷ **WHAT SHIPPED · 6 FEATURES** most completely described first ? what's the number?

01 **JavaScript/TypeScript and hybrid app code analysis** NEW 85

Scans code with Tree-sitter AST rules and detects frameworks including React Native, Expo, Cordova/Ionic, Capacitor and NativeScript. Decompiles Hermes bytecode files (`.bundle` , `.jsbundle` , `.hbc`) so AST rules, URL/domain extraction and secret scanning work on Hermes bundles, inspects hybrid app configuration via Cordova `config.xml` , Capacitor `capacitor.config.json` and Expo app config checks, discovers React Native `@ReactMethod` bridges, and adds a new View JavaScript source browser and JavaScript / Hybrid Code Analysis report section for Android and iOS.

— Names exact file types, frameworks, config files and report sections v4.6.6

02 **Windows APPX/MSIX in-process static analysis** NEW 85

Runs Windows APPX/MSIX static analysis in-process on any host, without requiring a Windows VM, BinSkim or BinScope. Checks PE binary hardening with `lief` for every packaged binary (ASLR, high entropy VA, DEP, CFG, SafeSEH, `/GS` , RWX sections, Authenticode, SDL banned APIs, including `.NET` IL-only assembly detection), analyses `AppxManifest.xml` capabilities and extensions and `AppxSignature.p7x` signer and publisher details for `.msix` , `.appxbundle` and `.msixbundle` formats, and detects strings, URLs, emails, secrets, malware domains and trackers inside the packages.

— Lists every hardening check, manifest file and package format v4.6.6

03 **Expanded iOS security checks** NEW 76

Analyses Entitlements and Provisioning Profile security for IPA and iOS source ZIP scans, applies modern iOS binary rules covering insecure TLS validation, weak Keychain accessibility, `WKWebView` file access, UIPasteboard and raw SQLite API use, performs cross-platform `lief` Objective-C/Swift class dumps, and checks iOS `Info.plist` file-sharing settings and tracker detection from embedded `.framework` bundles.

— Names specific APIs, files and checks covered v4.6.6

04 **Rate-limited threat database updates** IMPROVED 73

The `MOBSF_DB_UPDATE_INTERVAL` setting (default 1 hour) rate-limits Maltrail and Trackers DB update checks so scans no longer re-download threat databases on every run.

Avoid repeated database re-downloads on busy scan servers by increasing the update interval to 6 hours.

```env
MOBSF_DB_UPDATE_INTERVAL=360
```

— Exact config key, default value and runnable example given v4.6.6

THINNER COVERAGE BELOW

05 **URLhaus malware domain and IP lookups** NEW 25

Malware domains and IPs are now checked against URLhaus alongside existing Maltrail lookups.

— Names the integration but no mechanism or scope v4.6.6

06 **Flutter project source ZIP scanning** NEW 23

MobSF can now scan Flutter project source ZIP files.

— Bare capability name, no detail on checks performed v4.6.6

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

sslscan

Feedback ⓘ 2.2.4 NOTES ↗ RANK

sslscan tests SSL/TLS enabled services to discover supported cipher suites

> sslscan 2.2.4 adds a visual warning for an obsolete post-quantum key exchange group in scan output.

└──▷ WHAT SHIPPED · 1 FEATURE most completely described first ? what's the number?

01 **Obsolete post-quantum group flagged in output** IMPROVED

45

sslscan now flags `X25519Kyber768Draft00` in yellow in scan output to indicate it is an obsolete post-quantum key exchange group.

— Names exact group but no further mechanism detail 2.2.4

WAS THIS USEFUL? 👍 👎

Cure53 DOMPurify

Feedback ⓘ 3.4.18 NOTES ↗ RANK

DOMPurify - a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMPurify works with a secure default, but offers a lot of configurability and hooks. Demo:

> DOMPurify 3.4.18 adds a runtime warning to help catch a common misconfiguration when combining profile-based and explicit allowlist options.

└──▷ WHAT SHIPPED · 1 FEATURE most completely described first ? what's the number?

01 **Warning for USE_PROFILES combined with allowlists** IMPROVED

45

DOMPurify now logs a console warning when `USE_PROFILES` is combined with `ALLOWED_TAGS` or `ALLOWED_ATTR`, catching a likely misconfiguration at runtime.

— Names exact config keys but no example of the warning text 3.4.18

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Email Security

Abnormal AI

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗

Abnormal AI is a behavioral AI security platform that protects email, identity, and AI—and stops insider threats. Trusted by 5,000 organizations.

Abnormal AI adds an AI investigation agent to Identity Threat Protection that re-evaluates cases, can raise low-confidence compromises to medium, and produces downloadable PDF Case Reports.

Identity Threat Protection now includes an AI investigation agent that reviews user activity — including non-interactive sign-ins, email, and admin changes — after each detection, pulling signals the initial detection did not weigh.

The AI agent can raise a case from low to medium confidence when investigation supports it, triggering existing auto-remediation workflows if configured for medium-confidence cases.

Case promotion is added to the case timeline with a plain-language explanation drawn from the agent's investigation.

A Case Report consolidates the agent's verdict, key evidence, timeline, and primary indicators of compromise (IOCs) in one view, downloadable as a PDF from the case view.

UPDATED DETECTION QR code detection — animated GIF frame splitting

UPDATED DETECTION QR code and text scanning — images and PDFs inside .eml attachments

WAS THIS USEFUL? 👍 👎

◆ Network Analysis & Monitoring

Netcap

Feedback ⓘ v0.16.6 NOTES ↗ CODE ↗ RANK

Netcap is a framework for secure and scalable network traffic analysis - https://netcap.io

> Netcap v0.16.6 expands link-layer decoding, ties LDAP host records into its identity resolution, tightens C2 beacon corroboration, adds an NBNS parser, and fixes a stdin overwrite prompt.

└──▷ **WHAT SHIPPED · 5 FEATURES** most completely described first ? what's the number?

01 **LDAP host matching via directoryMatches** NEW 78

Adds `directoryMatches` to `Hosts.json` entries, linking LDAP computer objects whose name equals a host's observed name, and treats a bare name and its FQDN (e.g. `web01` and `web01.corp.example`) as one identity instead of flagging `conflicting-observations`.

– Names config field, file and exact before/after behaviour v0.16.6

02 **New link-type decoders for DLT 108, 50, 117, 119** NEW 68

Adds support for link types DLT 108 (OpenBSD loopback), DLT 50 (PPP in HDLC), DLT 117 (PFLog) and DLT 119 (Prism), and now routes PPP frames with the `0xff03` prefix, including DLT 9, through to transport decoders.

– Names exact DLT numbers and prefix but no further mechanism v0.16.6

03 **Corroborated c2.beacon detection** IMPROVED 68

Offline `c2.beacon` rows now carry `corroborated-by:<RecordType>` when both the TCP-timing and HTTP-timing detectors agree on the same source, destination and port.

– Explains mechanism and field but no usage example v0.16.6

04 **NBNS node-status decoder** NEW 65

Decodes NBNS node-status (type 0x21) responses with a dedicated parser, so captures with only NBSTAT traffic now produce `NBNS.ncap.gz`.

– Names type code and output file, no deeper mechanism v0.16.6

05 **Stdin overwrite prompt fix** IMPROVED 62

Non-terminal stdin with a non-empty output directory and no `-y` flag now fails with a clear `pass -y to overwrite` error instead of printing an unanswerable `Overwrite? [Y/n]:` prompt.

— Names exact flag and error message, clear before/after v0.16.6

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Plerion Feedback ⓘ

See your identity risk across every cloud in one place: NOTES ↗

Plerion is a cloud security platform that provides comprehensive risk management, vulnerability detection, and threat prioritization across cloud environments and workloads.

Plerion adds an Identity security dashboard for tracking open identity findings over time and prioritising them by Plerion rank across AWS, Azure, and GCP.

NEW DETECTION New Identity security dashboard shows identity risk across AWS, Azure, and GCP, covering admin privileges, external or cross-account access, privilege escalation paths, long-lived credentials, and inactive identities.

Track open identity findings over time and start with the findings Plerion ranks highest.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Huntress

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗ RANK

Give feedback to the Huntress team so we can make more informed product decisions. Powered by Canny.

> Huntress shipped a new Trials API for managing product trials programmatically, alongside improved visibility and recovery options for pending user invitations.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **Trials API for accounts and resellers** NEW 60

A new Trials API lets accounts and resellers list active and expired product trials, and choose which trials to start when creating accounts via the API.

— Describes endpoints' purpose but no exact paths given changelog-20261115-8dafb65f

02 **Invitation delivery status on Pending Users page** NEW 60

Admins can now view invitation delivery status — Sending, Delivered, Bounced, or Blocked — on the Pending Users page, with hover tooltips explaining each status and recommended next steps. Admins can also resend a Bounced invitation directly from the portal after confirming the recipient's mailbox is ready.

— Clear UI location and statuses named, no screenshot provided

changelog-20261115-8dafb65f

WAS THIS USEFUL? 👍 👎

XFA

Feedback ⓘ Application checks and AI checks NOTES ↗

XFA adds application checks and AI checks (beta, Max and Enterprise plans), with employee-controlled sharing of results with the organization.

NEW DETECTION Application safety check

NEW DETECTION Install protection check

NEW DETECTION Risky app categories check

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Backup & Recovery

Veeam Kasten

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗

RANK

Kasten K10 is a veeam Kasten is a Kubernetes-native platform for backing up, restoring, and migrating containerized applications and their persistent data.

> Kasten K10 added HTTP(S) proxy support for restricted-egress clusters and hardened file recovery, while also shipping several breaking changes to proxy behavior and deprecating three built-in Kanister Blueprints.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 HTTP(S) proxy support for restricted-egress clusters NEW

88

Kasten K10 now supports routing backup and restore traffic through an HTTP(S) proxy for clusters with restricted egress. On OpenShift, setting `global.proxy.openshift.caCertsAutoExtraction=true` pulls CA certificates automatically from the cluster-wide proxy object, while `global.proxy.httpsProxy` configures the proxy endpoint via Helm.

Deploy Kasten K10 on OpenShift behind a TLS-intercepting proxy so CA certificates are pulled automatically from the cluster-wide proxy object — no manual cert configuration needed.

```
$ helm upgrade k10 kasten/k10 --namespace kasten-io \
  --set global.proxy.openshift.caCertsAutoExtraction=true \
  --set
global.proxy.httpsProxy=https://proxy.corp.example.com:3128
```

— Exact Helm flags and a runnable upgrade command are given. changelog-20261115-b0eb30b3

02 Veeam Backup & Replication transfers bypass proxy BREAKING

60

Data transfer to Veeam Backup & Replication repositories no longer uses the proxy and always connects directly. Exports, restores, and imports fail if cluster egress is limited to the proxy until direct access to the backup server is allowed.

— States before/after and the required egress change. changelog-20261115-b0eb30b3

03 Deprecated Kanister Blueprints for K8ssandra, Crunchy PGO, RDS PostgreSQL

DEPRECATED

60

The built-in Kanister Blueprints for K8ssandra, Crunchy PGO, and RDS PostgreSQL are deprecated and will be removed in a future release; migrate using KB4956.

— Names the affected blueprints and points to migration article KB4956.

changelog-20261115-b0eb30b3

THINNER COVERAGE BELOW

04 Stricter security for FileRecoverySession CR IMPROVED

45

The `FileRecoverySession` CR and file recovery pod now enforce stricter input validation, restrictive mount options, and a read-only SFTP service.

— Names the CR and mechanisms but gives no reader action. changelog-20261115-b0eb30b3

└──▷ BREAKING ON UPGRADE

! Data transfer to Veeam Backup & Replication repositories no longer uses the proxy and always connects directly — exports, restores, and imports fail if cluster egress is limited to the proxy until direct access to the backup server is allowed.

! The multi-cluster proxy no longer forwards the caller's session and authentication credentials to secondary clusters, no longer relays cookie-changing response headers, and no longer supports WebSocket and other protocol upgrades through the proxy.

! On OpenShift, the console plugin proxy's plain-HTTP listener (port 8080) is no longer reachable from the `openshift-console` namespace.

! The built-in Kanister Blueprints for K8ssandra, Crunchy PGO, and RDS PostgreSQL are deprecated and will be removed in a future release; migrate using KB4956.

WAS THIS USEFUL?  

◆ Data Security & DLP

Varonis

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗ RANK

Varonis connects data, AI, and threat detection into one complete security platform that allows companies to keep innovating, without increasing risk.

> Varonis expanded its Atlas AI security platform with new gateways for controlling AI agent and LLM usage, plus browser-level protection against risky AI interactions.

└──▷ **WHAT SHIPPED · 4 FEATURES** most completely described first ? what's the number?

01 **LLM Gateway for model usage and cost control** NEW 75

The LLM Gateway tracks AI model usage and costs across more than 95 providers and 3,000 models, with granular policies to set model and token limits per user, group, or use case, and model-to-task policies specifying which models are allowed for specific workflows.

– Concrete numbers and policy scopes but no exact config name changelog-20261115-82c833e6

02 **Browser Protection for AI interactions** NEW 64

Varonis Browser Protection extends Atlas AI security to the browser, monitoring prompts, responses, and uploads in real time, redacting sensitive content before it reaches an AI provider, blocking unwanted interactions, and providing full session visibility including identities, policy violations, and enforcement actions.

– Explains behavior but lacks setup or flag detail changelog-20261115-82c833e6

03 **MCP Gateway for AI agent tool access** NEW 60

The MCP Gateway lets teams control which tools, APIs, and applications AI agents and MCP servers can reach, using identity-aware policies that tie every tool call to a real user identity and record it in an investigation timeline.

– Describes mechanism but no config surface named changelog-20261115-82c833e6

THINNER COVERAGE BELOW

04 **Agent Manifest in Atlas AI** NEW 10

Varonis added an Agent Manifest capability to its Atlas AI platform, but the changelog provides no further description of what it does.

– Named only in summary, no description given changelog-20261115-82c833e6

WAS THIS USEFUL?  

◆ Identity & Access Management

mock-oauth2-server

Feedback ⓘ 7.0.0 NOTES ↗ RANK

Mock OAuth2/OpenID Connect server for JVM tests and Docker Compose. No security workarounds needed.

> mock-oauth2-server 7.0.0 adds classpath-based loading of login pages and static assets, tightens OAuth 2.0 client enforcement across authorization code redemption, token refresh and revocation, and swaps its transitive logging dependency to a new package namespace.

└──▷ **WHAT SHIPPED · 5 FEATURES** most completely described first ? what's the number?

01 Client authentication enforcement on token revocation

80

BREAKING

Token revocation now requires client authentication or, for public clients, a `client_id` — sending only `token` returns `401 invalid_client`. Revoking a token with an identified client other than the one that obtained it now returns an empty `200` but leaves the refresh token valid.

— Two concrete scenarios with exact status codes documented 7.0.0

02 Classpath-based login page and static assets NEW

75

Login pages and static assets can now be loaded from the classpath by setting `classpath:login.html` or `classpath:static` in the existing path settings, alongside existing file-path support. This works for test resources, plain jars, and Spring Boot fat jars, letting a custom login page be bundled inside a jar without unpacking it to the filesystem.

Serve a custom login page bundled inside a Spring Boot fat jar or on the test classpath without unpacking it to the filesystem.

```text
classpath:login.html
```

— Names the exact config values and packaging scenarios supported 7.0.0

03 Client and redirect_uri enforcement on code redemption

75

BREAKING

Authorization code redemption now requires the same `client_id` and, if one was supplied at authorization, the exact same `redirect_uri`; a mismatch returns `400`

`invalid_grant` and consumes the code.

— Exact error code and consequence given, no runnable step `7.0.0`

04 **Client ownership enforcement on token refresh** BREAKING

75

Token refresh now requires the same client that originally obtained the token — a different client receives `400 invalid_grant`, and rotated tokens keep their original owner.

— Clear before/after with error code but no direct action `7.0.0`

05 **kotlin-logging dependency package change** BREAKING

70

The transitive `kotlin-logging` dependency is now `io.github.oshai:kotlin-logging-jvm` 8.0.7, using package `io.github.oshai.kotlinlogging.*` instead of `mu.*` — consumers must update imports or declare the legacy dependency explicitly.

— Exact package names, version, and migration note given `7.0.0`

└──▷ **BREAKING ON UPGRADE**

! Authorization code redemption now requires the same `client_id` and, if supplied at authorization, the exact same `redirect_uri` — a mismatch returns `400 invalid_grant` and consumes the code.

! Token refresh now requires the same client that obtained the token — a different client receives `400 invalid_grant`; rotated tokens keep the original owner.

! Token revocation now requires client authentication or, for public clients, a `client_id` — sending only `token` now returns `401 invalid_client`.

! Revoking a token with an identified client other than the one that obtained it returns an empty `200` but leaves the refresh token valid.

! The transitive `kotlin-logging` dependency is now `io.github.oshai:kotlin-logging-jvm` 8.0.7 with package `io.github.oshai.kotlinlogging.*` instead of `mu.*` — update imports or declare the legacy dependency explicitly.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Compliance Automation & Trust Management

Compyl

Feedback ⓘ changelog · Nov 15, 2026 CHANGELOG ↗ RANK

Compyl is the AI-powered GRC platform that maps one control library to SOC 2, ISO 27001, HIPAA, PCI DSS and 70+ frameworks, so you stay audit-ready year-round.

> Compyl's latest release lets users cancel in-progress integration syncs via a new Active Syncs panel, and reworks the reporting experience with a read-only Viewer and separate Designer mode.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **Cancel syncs with Active Syncs panel** NEW 80

Users can cancel a running or queued sync directly from the Integrations page; a running sync stops at its next saved step with already-pulled rows preserved, and a queued sync is simply removed from the queue. A new Active Syncs panel shows running, queued, stale, and cancelling syncs with live timers.

Stop a long-running sync mid-flight without losing already-pulled rows — useful when a large asset sync is blocking other work.

> 📍 In the Integrations page, open the Active Syncs panel, locate the running or queued sync, and click Cancel. The sync stops at its next saved step; rows already pulled are preserved and queued syncs are removed from the queue.

— Exact UI flow and sync-state behaviour given changelog-20261115-919be71d

THINNER COVERAGE BELOW

02 **Reports Viewer and Designer split** IMPROVED 55

Reports now open in a read-only Viewer by default, with a header toggle to switch to the editable Designer. Admins get separate links for each mode, and old report designer bookmarks redirect automatically to the new structure.

— Describes behaviour but no exact URLs or paths changelog-20261115-919be71d

WAS THIS USEFUL? 👍 👎

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ v4.3.1 NOTES ↗ RANK

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 200+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

> CISO Assistant adds a new compliance framework and polishes task display in this release.

└──▷ **WHAT SHIPPED · 2 FEATURES** most completely described first ? what's the number?

01 **ISO 9001:2015 framework support** NEW — 60

Adds an ISO 9001:2015 quality management systems framework outline, available in English and French, delivered via `iso9001-2015.yaml`.

– Names exact file and languages but no mapping detail v4.3.1

THINNER COVERAGE BELOW

02 **Improved task display** IMPROVED — 5

CISO Assistant now renders tasks with improved display.

– Vague, no mechanism or UI path given v4.3.1

WAS THIS USEFUL? 👍 👎

AGENT

◆ Agent Sandboxes

NoLabs nono

Feedback ⓘ v0.82.0 NOTES ↗ CODE ↗ RANK

The nono runtime runs AI agents in isolated environments with policy-controlled filesystem, network, and credential access.

> nono v0.82.0 adds OAuth device-flow platform login and a reorganized platform command, session terminal recording with replay/transcript playback, several new approval mechanisms in `nono proxy`, AWS operation-level endpoint policy matching and routing improvements for `aws_auth`, and a `remote` command group that replaces the removed `connect` subcommand.

└──▷ **WHAT SHIPPED · 8 FEATURES** most completely described first ? what's the number?

01 **AWS operation-level endpoint policy matching** NEW 85

Adds an `operations` field to `EndpointRuleConfig` so `endpoint_policy` on `aws_auth` routes can match specific AWS operation-name globs, letting a credential grant be restricted to named API actions such as `s3:GetObject`.

Restrict an AWS credential grant so the agent can only call specific S3 operations, not arbitrary API actions.

yaml

```yaml
operations:
  - s3:GetObject
  - s3:PutObject
```

— Config key and field named with a working YAML example v0.82.0

02 **Session terminal recording and playback** NEW 80

Adds session terminal recording (NEP-0010) so agent sessions are captured for later review, along with `nono replay` and `nono transcript` commands to play back or print a session's terminal recording.

Review what an agent did during a session by printing its terminal recording as text.

```
$ nono transcript <session-id>
```

— Names spec, two commands, and a runnable example v0.82.0

03 **Platform login and enrollment commands** NEW 70

Adds `nono login` and `nono logout` commands for OAuth 2.0 device-flow authentication and platform enrollment, and unifies platform commands under a reorganized `platform` command with automatic enrollment.

Authenticate with the nono platform using device-flow OAuth before accessing remote sessions or audit delivery.

```
$ nono login
```

— Names exact commands and auth flow with a runnable example v0.82.0

04 **New approval mechanisms in nono proxy** NEW 70

`nono proxy` gains a Unix-socket webhook transport for approval backends enabling local out-of-process approval daemons over `AF_UNIX` pathname sockets, approval elevation for `AF_UNIX` pathname socket connect and bind operations on Linux, a network approval flow for plain-HTTP forward requests, and approvals for `allow_domain` endpoints.

— Names every approval surface but no runnable example given v0.82.0

05 **aws_auth routing improvements** IMPROVED 70

Improves `aws_auth` routing by selecting the signing profile via placeholder access key ID, deriving the signing region from the request host for wildcard upstream configurations, and accepting AWS GovCloud regions and S3 bucket-subdomain wildcards in `aws_auth` proxy routes.

— Names several concrete routing behaviors, no runnable example v0.82.0

06 **Remote session command group replaces connect** BREAKING 60

Adds a `remote` command group to launch, list, and connect to remote sessions; the `connect` subcommand is removed, with remote session connectivity now under the `remote` command group.

— Names removed and replacement commands, no exact syntax shown v0.82.0

THINNER COVERAGE BELOW

07 **Custom phantom-token format control** NEW 45

Adds `phantom_format` to custom credentials configuration to control token format for phantom-token injection.

— Names the field but gives no mechanism detail or example v0.82.0

08 **Live proxy audit event logging** IMPROVED 35

Proxy audit events are now recorded live to the audit log as they occur, rather than only at session finalization.

— States before/after but no config surface named v0.82.0

└──▷ **BREAKING ON UPGRADE**

! The `connect` subcommand is removed; remote session connectivity is now under the `remote` command group.

WAS THIS USEFUL?  

GOVERN

◆ Model & Agent Protection

Minimal Software Research minimal

Feedback ⓘ

release-a42a9d6d NOTES ↗ RANK

Minimal is a secure, declarative runtimes for Claude Code, Gemini, Codex, Pi and more, so you can run multiple agents safely on your stack from a verified software supply chain.

> minimal's single release in this window adds a Box Egress Proxy with client-key limits, a named-secret store, opt-in OpenTelemetry tracing, and a cluster of new CLI commands covering box audit trails, GitHub login, and security diagnostics.

└──▷ **WHAT SHIPPED · 6 FEATURES** most completely described first ? what's the number?

01 **Egress controls for Box Egress Proxy and runs** NEW — 70

The Box Egress Proxy gains `bep serve --max-client-keys` to set the client-key bound, and `min task run` / `min box run` take new network and egress flags to control network access during runs.

— Names flag and commands but egress flags unspecified. release-a42a9d6d

02 **GitHub login and logout flow** NEW — 65

`min login` signs in to GitHub, finishing on a real page with repository choice; logging out deletes the stored sign-in and refuses every reference to it afterward.

— Describes flow and command but no flags shown. release-a42a9d6d

03 **Named secret storage via min secret** NEW — 65

`min secret` stores named secrets, for example `min secret set GH_TOKEN`, so a box can retrieve a credential without it being pasted at session start.

Store a GitHub token as a named secret so a box can retrieve it without you pasting it at session start.

```
$ min secret set GH_TOKEN
```

— Runnable example command grounds the capability. release-a42a9d6d

04 **OpenTelemetry tracing with local spool** NEW — 65

minimal adds opt-in OpenTelemetry export with a local spool via `mlog`, emitting one trace per request across both `min` and `minimald`.

— Mechanism named but no exact enable command shown. release-a42a9d6d

THINNER COVERAGE BELOW

05 **Security diagnostics reporting** NEW 45

`min diag --security` sends a suspected vulnerability report.

— Single command, no further mechanism given. release-a42a9d6d

06 **QUIC block helper named in installer** NEW 35

`min finalize-install` now names the QUIC block helper.

— Thin one-line description with no further detail. release-a42a9d6d

└──▷ ALSO FROM THESE RELEASES

Export a box's current spec as JSON for scripting or audit pipelines.

```
$ min box show -o json mybox
```

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · November 15, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue