THE CYBER TOOLCHAIN

NO. 151

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED NOVEMBER 26, 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

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 146 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 44 of 47 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: Sysdig Secure makes cloud exposure validation self-service, Qualys TotalCloud brings AI service

vim ? help

inventory and red-teaming into one module, and GitHub CLI now revokes tokens on logout instead of just forgetting them locally.

PROTECT

Turn on cloud exposure validation without a support ticket

Validated Exposure can now be enabled for AWS, GCP, and Azure accounts from the UI or infrastructure-as-code. That removes the vendor handoff from rollout, so teams can test whether exposed cloud paths are actually exploitable as part of their own deployment workflow.

Sysdig Secure

IDENTIFY

Build an inventory of AI services before securing them

TotalAI adds AI service inventory alongside model red-teaming, MCP server and CI/CD secret scanning, and AI-aware identity and network monitoring. The immediate gain is knowing where AI systems and supporting interfaces exist, instead of treating them as unmanaged exceptions outside normal cloud risk work.

Qualys TotalCloud

PROTECT

Revoke GitHub CLI credentials when users log out

`gh auth logout` now revokes the OAuth token and clears saved Git credentials by default, with an opt-out for local-only logout. That closes the common gap where a machine forgets a credential but the token remains valid server-side.

GitHub CLI

GOVERN

Review access by profile instead of only by application or entitlement

Governance campaigns can now scope reviews to access profiles, with conditional logic and regex validation available in request forms. That lets reviewers certify a business access bundle as a unit, reducing the spreadsheet work of reconstructing which individual grants belong together.

ConductorOne

Does **GPT-5.5** read better? 👍 👎

◆ Autonomous Offensive Frameworks (AOF)

Hacktron

Feedback ⓘ changelog · Nov 26, 2026 CHANGELOG ↗ RANK

Hacktron is a review, Whitebox, the API, and MCP.

> Hacktron's latest release adds a signed Webhook notifier for automations, a Fix column for triaging findings, multi-application repository membership, and clearer cost and scope visibility across scans and reports.

└──▷ **WHAT SHIPPED · 9 FEATURES** most completely described first ? what's the number?

01 Webhook notifier for automations

Not checked yet NEW

77

A new Webhook notifier posts signed JSON events to an HTTPS endpoint and records deliveries in run history; new-vulnerability automations can now notify without requiring an action to be configured. Set it up in Automations by editing an automation's Settings tab, adding a Webhook notifier, entering the HTTPS endpoint URL, and setting the trigger to New vulnerability while leaving Actions empty.

Receive instant alerts in your incident pipeline when Hacktron discovers a new vulnerability, without needing to configure a remediation action first.

> 📍 In Automations, create or edit an automation, open the Settings tab, add a Webhook notifier, enter your HTTPS endpoint URL, and set the trigger to New vulnerability — leaving the Actions section empty.

— Names mechanism and exact setup steps, missing payload schema.

changelog-20261126-5ef43d12

02 Delete finished scans from scans list

Not checked yet NEW

60

A finished scan and its report can now be removed via Delete scan in the scans list menu, while its findings remain in Findings.

Remove a completed scan and its report to keep the scans list tidy while preserving all associated findings for ongoing triage.

> 📍 In the Scans list, locate the finished scan, open its menu, and select Delete scan — the scan and report are removed but its findings remain in Findings.

— Exact control name and steps to use it. changelog-20261126-5ef43d12

THINNER COVERAGE BELOW

03 **Fix column in findings list** Not checked yet NEW 55

A new Fix column on the findings list shows View fix when a fix is in review, or a request-fix button on hover for open findings without one.

Quickly triage which open findings already have a fix available versus those still awaiting one, without opening each finding individually.

> 📍 In the Findings list, locate the Fix column: findings showing View fix have a fix in review; hover over open findings without one to request a fix.

— Clear UI behaviour and navigation, no deeper mechanism given.

changelog-20261126-5ef43d12

---

04 **Per-repository cost estimates for pentests** Not checked yet

IMPROVED 55

Cost estimates now quote the whole pentest by code size and show each repository's lines of code, with an expandable folder breakdown of Lines and Credits.

— Describes what changed but not where to view it. changelog-20261126-5ef43d12

---

05 **Code scope visibility in scans and PDF reports** Not checked yet

NEW 53

Scan details now show a Code scope panel with each repository's include and exclude rules, and Full and Executive PDF reports include a Paths in scope table reflecting the same scope.

— Names the panel and table but no navigation steps given. changelog-20261126-5ef43d12

---

06 **Multi-application repository membership** Not checked yet NEW

50

Repositories can now belong to several applications, and repository pickers — including Add context — show every application they belong to, with a +N badge on hover.

— Names the picker and badge behaviour, no step-by-step flow. changelog-20261126-5ef43d12

---

07 **Inactive findings stay visible with undo** Not checked yet IMPROVED

48

Findings moved to an inactive status now stay visible and dimmed, with an Undo option in a Moved to inactive toast, and the findings list no longer applies a default Status filter.

— Describes behaviour change fully but no usage walkthrough. changelog-20261126-5ef43d12

---

08 **Default organisation on sign-in** Not checked yet NEW 42

Users can set a default organisation to open after sign-in using Set as default in personal settings.

— Names the exact control and where to find it. changelog-20261126-5ef43d12

09 **Consistent finding IDs across app and PDF reports** Not checked yet

IMPROVED

25

Full and Executive PDF reports now use the same finding IDs as the app, aligning report references with the in-app findings list.

— Bare statement of the fix with no further detail. changelog-20261126-5ef43d12

WAS THIS USEFUL? 👍 👎

xalgorix

Feedback ⓘ v4.6.209 NOTES ↗ RANK

> xalgorix added subdomain exclusion controls for wildcard scans, letting users suppress specific hosts from expanding into full sub-scans at both the server and per-scan level.

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

01 Subdomain exclusion for wildcard scans

Not checked yet NEW

88

Set `XALGORIX_WILDCARD_EXCLUDE` (comma-separated, server-wide, via env var or Settings → Runtime) or pass the per-scan `exclude_subdomains` list on a scan request to suppress hosts like dev, staging, or QA from being expanded into full sub-scans; the two are merged at scan time. Matching supports plain DNS-label matching or glob syntax (`*` , `?`), e.g. `dev-*` , `*-qa` , or `*.internal.example.com` , applied before the wildcard subdomain cap, with excluded hosts reported in the scan activity feed.

Exclude dev, staging and QA hosts globally so they are never expanded into sub-scans on any wildcard engagement run on this server.

```
$ XALGORIX_WILDCARD_EXCLUDE=dev,staging,*-qa xalgorix --web
```

Suppress internal and staging subdomains for a single scan via the API, without changing server-wide settings.

```
$ curl -s -X POST http://127.0.0.1:9137/api/scans \
  -H 'Authorization: Bearer <token>' \
  -H 'Content-Type: application/json' \
  -d '{"target": "*.example.com", "exclude_subdomains":
["staging", "dev", "*.internal.example.com"]}'
```

— Names exact env var, field, glob syntax and runnable examples v4.6.209

WAS THIS USEFUL? 👍 👎

◆ Hacking Hardware

O.MG / Hak5 O.MG Cable Feedback ⓘ

back in stock · Nov 25, 2026 STORE ↗

O.MG Cable is a hand-made USB cable with a WiFi-controlled implant hidden inside that injects keystrokes, so red teams can emulate sophisticated physical attacks.

Basic, USB-A to USB-C (Black TPE) (omg-cable-basic-usba-usbc-black) back in stock at `shop.hak5.org` on 25 Nov 2026. Not checked yet

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Secrets Detection & Management

GitGuardian Detection Engine

Feedback ⓘ

changelog · Nov 26, 2026 CHANGELOG ↗

GitGuardian Detection Engine scans code repositories and developer workflows to automatically detect exposed secrets, API keys, and credentials in real time.

NEW DETECTION CrowdSec LAPI Secret detector

NEW DETECTION Deno Deploy organization token detector: Deno Organization Token

NEW DETECTION GAP Cloud agent token detector: GAP Agent Token

NEW DETECTION IBM Instana API token detector

NEW DETECTION Idira Adaptive Authentication detector

NEW DETECTION Lovable API key detector

NEW DETECTION Qdrant API key detector

NEW DETECTION LINE Messaging API channel credentials checker: Line Messaging OAuth2 Keys

NEW DETECTION Analyzers for 26 secret types: Confluent, GitHub Enterprise, Google Cloud OAuth2 access tokens, Heroku, HubSpot and 14 more

NEW DETECTION Auth0 revoker

NEW DETECTION Supabase service_role JWT revoker

UPDATED DETECTION Alchemy API key detector prefix update

UPDATED DETECTION HashiCorp Consul ACL token detector instance URL capture

UPDATED DETECTION PostHog personal API key detector current format support

UPDATED DETECTION IBM Cloud key analyzer enrichment

UPDATED DETECTION Cloudant IAM analyzer account owner enrichment

NEW DETECTION Nine new detectors: age private keys, Microsoft Entra refresh tokens, GitHub App refresh tokens, keystore passwords, and five Oracle Cloud Infrastructure credential types: Azure Entra Refresh Token, Oracle Cloud Infrastructure API Signing Key, Oracle Cloud Infrastructure Auth Token, Oracle Cloud Infrastructure Customer Secret Key, Oracle Cloud Infrastructure OAuth 2.0 Client Credentials and 1 more

NEW DETECTION Nine new analyzers: Azure Active Directory, Azure Container Registry, Codacy, DeepL, Dropbox, Eventbrite: Codacy API, Codacy project tokens, DeepL Free, DeepL Pro, Dropbox access tokens and 1 more

UPDATED DETECTION PayPal OAuth2 detector now finds client_id:client_secret pairs: PayPal OAuth2 Keys

UPDATED DETECTION ibm_platform_api_key recall increase

WAS THIS USEFUL?  

infisical

Feedback ⓘ v0.167.16 NOTES ↗ RANK

Infisical is an open-source secret management platform that helps teams securely store, sync, and manage API keys, environment variables, and other sensitive credentials.

> Infisical v0.167.16 adds Microsoft Autoenrollment and new revocation logic to PKI, real-time audit streaming and a CLI to PAM, and rounds out the release with gateway downtime alerts, recursive folder permissions, and several smaller platform refinements.

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

01 **Secret import endpoint field and policy enforcement**

Not checked yet IMPROVED 70

The GET endpoint for secret imports now exposes an `importEnv.projectId` field identifying the source project of an imported secret, and secret imports now respect change policies so approval workflows apply to imported secrets.

– Field named but exact endpoint path not given v0.167.16

02 **PKI certificate SAN, Microsoft Autoenrollment, and auto-revocation**

Not checked yet NEW 60

PKI certificate policies now support adding the common name as a DNS SAN. PKI also supports Microsoft Autoenrollment as a new enrollment method, and automatically revokes local signers when DigiCert revokes their certificate.

– Three PKI mechanisms named, no config keys given v0.167.16

03 **PAM audit streaming, approver toggle, and CLI** Not checked yet

NEW 60

PAM now streams session activity to audit log streams in real time, adds a per-folder approver email toggle for PAM workflows, and adds an agent-friendly CLI for PAM.

– Three PAM additions named but no commands or flags given v0.167.16

THINNER COVERAGE BELOW

04 **AWS account reporting on instance details page** Not checked yet

NEW 45

Infisical now reports the AWS account it runs as on the instance details page.

– Names exact UI location, minimal mechanism v0.167.16

05 **Gateway downtime alerts** Not checked yet NEW 35

Gateway downtime now triggers alerts through the shared alerting module.

— Brief mention, no configuration detail given v0.167.16

06 **Renewal payment failure banner** Not checked yet NEW 25

Org members now see a banner when a renewal payment fails.

— Thin one-line description, no further detail v0.167.16

WAS THIS USEFUL? 👍 👎

GitGuardian SaaS Feedback ⓘ

NHI Governance now accessible on every plan, free for up to 500 secrets (2026-11-25)

BLOG ↗

GitGuardian SaaS is a secrets detection platform that scans Git repositories and developer workflows to identify and remediate exposed API keys, credentials, and sensitive data.

NHI Governance is now on every plan: free inventory of up to 500 secrets via `ggscout`, with policies, ownership and push-to-vault included. Growth raises limits to 5,000 secrets and 5,000 identities.

Connect HashiCorp Vault, AWS Secrets Manager, Azure Key Vault and other secrets managers via `ggscout` on every plan, with free inventory of up to 500 secrets and no time limit on the Free plan. Not checked yet

Use `ggscout` 0.35.0 or later to see which sources your current plan accepts before connecting. Not checked yet

Every plan now includes security policies, ownership assignment and push-to-vault capabilities in NHI Governance. Not checked yet

A 30-day trial at Growth limits starts automatically when a Free plan account reaches 500 secrets; on expiry the inventory retains the 500 oldest secrets and the rest returns on upgrade. Not checked yet

NEW INTEGRATION NHI Governance — Kubernetes and CI/CD sources

UPDATED INTEGRATION SharePoint Online Multi-Geo tenant scanning: Microsoft 365

WAS THIS USEFUL? 👍 👎

◆ Code Security

Semgrep

Feedback ⓘ updated · Nov 26, 2026 NOTES ↗ RANK

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

> Semgrep's single release this window centers on tighter Guardian governance and Supply Chain visibility, adding org-wide observe-only mode, npm private registry Autofix support, MCP-based project archiving, threat-grouped advisories, and a Secrets file-reveal option, alongside several breaking changes to the Autofix API and Supply Chain reachability classification.

└──▷ **WHAT SHIPPED · 12 FEATURES** most completely described first ? what's the number?

01 Org-wide Guardian observe-only mode

Not checked yet NEW

80

Enable Guardian observe-only mode organization-wide with the Guardian observe-only mode setting in `Settings > General > Global`, replacing the per-machine `SEMGREP_GUARDIAN_OBSERVE_ONLY` environment variable. Requires Guardian 2.10.63 or later; in this mode Guardian scans and reports findings to AppSec Platform without surfacing them to developers or blocking coding agents.

Turn on Guardian observe-only mode org-wide so Guardian scans and reports findings to AppSec Platform without surfacing them to developers or blocking coding agents.

📍 In the Semgrep web console, go to Settings › General › Global and enable the Guardian observe-only mode toggle. Ensure all developer machines are running Guardian 2.10.63 or later.

— Exact setting path, replaced env var, and version requirement given snapshot-20261126

02 Secrets finding source file reveal

Not checked yet NEW

70

Semgrep Secrets finding details can now reveal the source file containing a secret — click Show file to fetch it from your source code manager. The file is hidden by default and Semgrep does not store it.

Reveal the source file for a Semgrep Secrets finding to confirm the leaked credential's exact location without Semgrep storing the file.

📍 Open a Semgrep Secrets finding in the Findings page, then click Show file in the finding details panel to fetch the file from your source code manager.

— Exact control named with clear privacy behaviour and usage steps snapshot-20261126

03 **Supply Chain reachability reclassification** Not checked yet

70

BREAKING

Supply Chain no longer marks transitive dependency findings as Unreachable when reachability has not been analyzed — these now appear as No reachability analysis under Needs review. Previously Unreachable findings will be reclassified, the default provisional ignore automation will no longer apply to them, and reachability filters and counts may differ from finding details for a few days during the transition.

— Clear before/after states named with transition caveat snapshot-20261126

---

04 **Threat-grouped Supply Chain advisories** Not checked yet IMPROVED

65

Supply Chain's Advisories page now groups advisories by threat — use Group & sort to group By threat or By advisory and sort By created date or By number of findings, with search now matching threat names and the start of advisory IDs.

— Named UI controls give a clear starting point, no deeper mechanism snapshot-20261126

---

05 **npm private registry for Supply Chain Autofix** Not checked yet

NEW

60

Add an npm private registry in `Settings > Integrations > Registry` to get Supply Chain Autofix and upgrade guidance for private packages.

Register an npm private registry so Supply Chain Autofix and upgrade guidance work for internal packages.

> 📍 In the Semgrep web console, go to Settings › Integrations › Registry and add your npm private registry URL and credentials.

— UI path named but mechanism of autofix not detailed snapshot-20261126

---

06 **Detect-2Shell workflow extended to Java4Shell** Not checked yet

IMPROVED

60

The Detect-2Shell Agentic Workflow now also scans for repositories potentially affected by the Java4Shell vulnerability, checking JDK and JRE image tags, Dockerfiles, Kubernetes manifests, and Compose files.

— Scope of scanned artifacts is specific but no run command shown snapshot-20261126

THINNER COVERAGE BELOW

07 **Stricter Autofix API parameter validation** Not checked yet

55

BREAKING

Autofix API requests that pass different values for the same parameter across the path, body, or query are now rejected; previously the path value was used silently.

— Clear before/after behaviour but no endpoint name given snapshot-20261126

08 **MCP-based project archiving** Not checked yet NEW 50

Connect Semgrep Platform to a ChatGPT or Codex MCP client via the Semgrep plugin to archive or unarchive projects directly from the MCP client.

— Names clients and plugin but no setup steps given snapshot-20261126

09 **Expanded Julia parsing and matching** Not checked yet IMPROVED 50

Julia parsing and matching now support public declarations, outer-qualified loop bindings, typed const fields with no initial value in mutable structs, renamed macro imports (`import A: @m as @n`), expressions starting with `±` , binary `±` distinct from `∓` , and `where` constraints in function-definition patterns.

— Many named syntax cases but no usage example given snapshot-20261126

10 **Plan requirement for Wiz and Cortex connections** Not checked yet 50

BREAKING

New Wiz and Cortex connections now require a Semgrep Teams or Enterprise plan — existing connections on lower plans will no longer be created.

— Names integrations and plan tiers, no further mechanism snapshot-20261126

11 **Domain condition for remediation policies** Not checked yet NEW 40

Remediation policies triggered after an Agentic Workflows run can now use a Domain condition to filter issues by security or correctness.

— Names the condition but not how to configure it snapshot-20261126

12 **30-day scan history in Scans & Workflows tab** Not checked yet 35

IMPROVED

A project's Scans & Workflows tab now shows the last 30 days of scan history.

— Bare fact with a named UI location, no further mechanism snapshot-20261126

└──▷ **BREAKING ON UPGRADE**

! Autofix API requests that pass different values for the same parameter across the path, body, or query are now rejected; previously the path value was used silently.

! New Wiz and Cortex connections now require a Semgrep Teams or Enterprise plan — existing connections on lower plans will no longer be created.

! Supply Chain transitive dependency findings previously marked `Unreachable` will be reclassified to `No reachability analysis` under `Needs review`, and the default provisional ignore automation will no longer apply to them; reachability filters and counts may differ from finding details for a few days during the transition.

WAS THIS USEFUL? 👍 👎

OpenQodex

Feedback ⓘ openqodex@0.25.0 NOTES ↗ RANK

OpenQodex is a join the world's most widely adopted, AI-powered developer platform where millions of developers, businesses, and the largest open source community build software that advances humanity.

> OpenQodex 0.25.0 introduces anonymous telemetry with granular opt-out, makes per-repository agent reviews explicitly opt-in via a config file (a breaking change for existing repos), and adds an interactive reviewer-list confirmation step to `init`.

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

01 Anonymous telemetry with opt-out controls

Not checked yet NEW

86

Telemetry can be disabled by adding `openqodex_telemetry: 0` to `.openqodex/config.yaml`, or by setting `OPENQODEX_TELEMETRY=0` or `DO_NOT_TRACK=1` in the environment; it is always off in CI and when running with `--offline`. Run `openqodex guide telemetry` to list every field that gets sent.

Disable telemetry for a repository that handles sensitive code, using the config file.

yaml

```yaml
openqodex_telemetry: 0
```

— Names config key, two env vars, flag and inspection command openqodex@0.25.0

02 Per-repository opt-in for agent push-hook reviews

Not checked yet

77

BREAKING

Agent reviews are now activated per-repository by placing a `.openqodex/config.yaml` or `.openqodex.yaml` file at the repository root; Claude Code and Codex push hooks only run in repositories that have this settings file. This is a breaking change — repositories lacking the file no longer get push-hook reviews, so `openqodex init` must be run in each repository to opt it in.

— Names config files and affected hooks, clear migration path openqodex@0.25.0

03 Interactive reviewer-list confirmation in init

Not checked yet

IMPROVED

70

Running `openqodex init` now shows the planned reviewer list and asks for confirmation before writing it, letting you keep the order, change it, drop reviewers, or write no list at all; passing `--yes` skips the prompt as before.

Opt a repository into agent push-hook reviews and confirm the reviewer list interactively.

```
$ npx openqodex init
```

— Names command and flag with exact new behaviour `openqodex@0.25.0`

└──▷ **BREAKING ON UPGRADE**

! Agent push hooks (Claude Code and Codex) no longer run in any repository that lacks a `.openqodex/config.yaml` or `.openqodex.yaml` settings file; run `openqodex init` in each repository you want reviewed to create the file and opt it in.

WAS THIS USEFUL? 👍 👎

---

syzkaller

Feedback ⓘ changes since 2026-11-24 CODE ↗

Syzkaller is an unsupervised, coverage-guided kernel fuzzer developed by Google that automatically finds bugs in operating system kernels, primarily Linux.

syzkaller adds VMFUNC/EPTP-list support for x86 SYZOS and a `reproduce_only` manager config option

└──▷ **USE IT**

Cap a syz-manager instance to only reproduce existing crashes, skipping new fuzzing — useful for dedicated repro infrastructure.

```yaml
reproduce_only: true
```

Restrict fuzzing runs to reproduction only by setting `reproduce_only` in `pkg/mgrconfig`. Not checked yet

syzkaller adds VMFUNC support to x86 SYZOS via new `SYZOS_API_NESTED_INTEL_VMFUNC` and `SYZOS_API_NESTED_INTEL_EPTP_LIST_SET` API calls and a new `NESTED_PAGE_EPTP_LIST` page type. Not checked yet

---

WAS THIS USEFUL? 👍 👎

GitLab

Feedback ⓘ

Take on complex coding changes with Gemini 4 Neon on GitLab (2026-11-25) BLOG ↗

RANK

Teams and agents ship trusted software faster with GitLab, the intelligent orchestration platform with context and governance for the entire software lifecycle.

> GitLab added Gemini 4 Neon, a new coding-focused model to GitLab Duo Agent Platform, and gave admins the ability to assign different Gemini 4 models to different Duo Agent Platform features.

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

01 **Gemini 4 Neon coding model in Duo Agent Platform** Not checked yet

NEW 65

GitLab Duo Agent Platform now includes Gemini 4 Neon, a model built for agentic coding work such as planning issues, reading long specs, answering codebase questions in Agentic Chat, and carrying multi-file changes through to a merge request. The model completed 100% of benchmark tasks and resolved 76.7% end-to-end.

– Names benchmark numbers and use cases but no concrete command or UI path.

Take on complex coding changes with Gem…

THINNER COVERAGE BELOW

02 **Per-feature model selection across Gemini 4 variants**

Not checked yet NEW 55

Admins can now assign a different Gemini 4 model — Neon, Hydrogen, Carbon, or Argon — to different features within GitLab Duo Agent Platform, and change these assignments as often as needed, with the same context, policy checks, and audit trail applied across all models.

– Names the four models and governance behavior but not the admin workflow.

Take on complex coding changes with Gem…

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ SCM and ticketing (2026-11-25) BLOG ↗ RANK

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

> Veracode expanded its SCM/CI workflow integrations with new `veracode.yml` configuration options, platform-managed GitHub app installation and scan scheduling, while eLearning added OWASP Top 10:2025 courses in the European region and deprecated its REST API.

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

01 New veracode.yml config options for workflow integrations

Not checked yet NEW 85

Adds `predependency_command` to run single-line or multiline commands before Veracode packages a project (available in GitHub, GitLab, and Azure DevOps workflow integrations); `policy` for infrastructure-as-code (IaC) scans (GitHub, GitLab, Azure DevOps); `build_runs_on` for SCA scans in the GitHub Workflow Integration; a custom agent pool name parameter in the Azure DevOps Workflow Integration to specify the agent pool for pipeline execution; and `debug` for debugging and troubleshooting across GitHub, GitLab, and Azure DevOps workflow integrations.

— Names every flag and its scope but no usage example SCM and ticketing (2026-11-25)

02 Scan scheduling from Veracode Platform

Not checked yet NEW 75

Schedule Static Analysis, SCA, and IaC scans from the Veracode Platform for GitHub organizations, and schedule scans for every organization in which the Azure DevOps Workflow Integration is installed, driven by `veracode.yml` configuration. Also schedule scans for a specific `analysis_branch` in `veracode.yml` for the Azure DevOps Workflow Integration instead of always using the default branch.

— Names config key and scope, mechanism clear but no steps SCM and ticketing (2026-11-25)

03 Platform-managed GitHub Workflow Integration setup

Not checked yet NEW 65

Install, configure, and update the GitHub Workflow Integration directly from the Veracode Platform, replacing manual GitHub Marketplace steps; also adds autopackaging support for Apex, VB6, and Perl.

— Clear before/after and new languages, no exact UI path given

SCM and ticketing (2026-11-25)

04 OWASP Top 10:2025 eLearning courses in European region

Not checked yet NEW 60

Secure coding language addendum courses covering .NET, Java, JavaScript, PHP, and Python aligned to OWASP Top 10:2025 are now available in the European region in Chinese, English, French, Portuguese, and Spanish. The Software Security Awareness - OWASP Top 10:2025 course is now available in the European region in English, French, German, Japanese, Portuguese, and Spanish.

— Lists languages and topics but no access steps Veracode eLearning (2026-11-25)

THINNER COVERAGE BELOW

05 **eLearning report start date selection** Not checked yet IMPROVED 45

Select a report start date of up to one year in the past when generating eLearning reports.

— Gives concrete one-year limit, minimal mechanism detail Veracode eLearning (2026-11-25)

06 **GitHub app uninstallation workflow** Not checked yet NEW 40

Uninstall the Veracode app from GitHub organizations using a new uninstallation workflow on the Veracode Platform.

— Describes the action but no detail on mechanism SCM and ticketing (2026-11-25)

07 **Jira 11 support in Jira integration** Not checked yet IMPROVED 40

Veracode Integration for Jira Server now supports Jira 11, including Java 21 compatibility.

— States compatibility but no migration or setup detail SCM and ticketing (2026-11-25)

08 **eLearning REST API end of support** Not checked yet DEPRECATED 40

The Veracode eLearning REST API has reached end of support — it will no longer be updated or receive technical support.

— States end of support with no migration path given Veracode eLearning (2026-11-25)

└──▷ BREAKING ON UPGRADE

! The Veracode eLearning REST API has reached end of support — it will no longer be updated or receive technical support.

WAS THIS USEFUL? 👍 👎

◆ WAF, Bot & API Protection

fcaptcha

Feedback ⓘ v1.52.0 NOTES ↗ RANK

Fcaptcha is a self-hosted, invisible CAPTCHA that detects AI agents driving real browsers. 2 AA, and EAA: no cookies, no third-party data sharing, and no visual or audio puzzle.

> fcaptcha v1.52.0 adds new bot-detection signals — external-CDP telemetry, a canvas readback-stability score, and a JA4 browser-family identity axis — plus runnable SvelteKit and Remix integration examples.

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

01 **Canvas readback-stability signal** Not checked yet NEW

55

Adds a low-confidence canvas readback-stability signal that contributes `0.0112` to the score; it must be corroborated by other signals and is not a standalone blocking signal.

— Names exact score contribution and corroboration requirement v1.52.0

02 **JA4 browser-family identity axis** Not checked yet NEW

47

Adds a trusted/native JA4 browser-family identity axis with fail-open behavior for unknown or shared fingerprints.

— Names the signal and its fail-open behavior, no further mechanism v1.52.0

03 **SvelteKit and Remix integration examples** Not checked yet NEW

45

Adds runnable SvelteKit and Remix integration examples, with all demo and image pins updated to `1.52.0`.

— Names frameworks and version pin, but no code shown here v1.52.0

04 **External-CDP input-shape telemetry** Not checked yet NEW

43

Adds observe-only external-CDP input-shape telemetry for browser-agent research; this data collection does not affect production scores.

— Describes mechanism and scope but no config surface named v1.52.0

WAS THIS USEFUL? 👍 👎

Fastly

Feedback ⓘ Fastly Terraform Provider (beta) 0.2.11 (2026-11-24)

BLOG ↗ RANK

Fastly is a cloud edge computing platform that accelerates website and API performance through a global CDN, real-time caching, and security services.

> Fastly's beta Terraform provider adds a migration toolchain (`fastly-tf-migrate`) for moving legacy Compute, NGWAF, TLS/authentication logging, and domain configurations to new resource types, and introduces bot management resources and data sources.

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

01 Compute service migration to `fastly_service_compute_auto`

Not checked yet NEW 80

`fastly-tf-migrate` migrates legacy `fastly_service_compute` HCL configurations to the new `fastly_service_compute_auto` resource, with end-to-end test coverage runnable via `make test-migration-compute`.

Run the compute migration to convert a legacy `fastly_service_compute` configuration to `fastly_service_compute_auto` and validate end-to-end.

```
$ make test-migration-compute
```

— Names both resource types and gives a runnable test command.

Fastly Terraform Provider (beta) 0.2.11…

02 Syntax-aware reference rewriting during migrations

Not checked yet NEW 65

During legacy VCL and Compute service migrations, `fastly-tf-migrate` rewrites Terraform references syntax-aware, preserving module addresses, resource labels, `count`, `for_each`, provider aliases, and supported meta-arguments.

— Detailed mechanism and preserved elements, but no runnable example.

Fastly Terraform Provider (beta) 0.2.11…

03 TLS and auth config transformation for logging endpoints

Not checked yet NEW 65

`fastly-tf-migrate` transforms TLS and authentication configuration for HTTPS, Elasticsearch, Kafka, Splunk, and Syslog logging endpoints, preserving legacy VCL format defaults and HTTPS gzip-level state hints.

— Names five endpoint types and preserved behavior, no example.

Fastly Terraform Provider (beta) 0.2.11…

04 **Bot management resources and data sources** Not checked yet NEW

60

Adds `fastly_bot_management_bots` and `fastly_bot_management_categories` resources and data sources, letting Terraform retrieve stable, sorted lists of bots and categories for use in policy rules.

Declare bot management data sources to retrieve stable, sorted lists of bots and categories for use in policy rules.

```hcl
data "fastly_bot_management_bots" "bots" {}

data "fastly_bot_management_categories" "categories" {}
```

— Example HCL declaration shown for data sources.

Fastly Terraform Provider (beta) 0.2.11…

THINNER COVERAGE BELOW

05 **NGWAF resource state migration via moved blocks** Not checked yet

NEW

50

`fastly-tf-migrate` moves Terraform state from legacy NGWAF resources to their renamed and split resource types using Terraform `moved` blocks.

— Mechanism named but no example or exact resource names given.

Fastly Terraform Provider (beta) 0.2.11…

06 **Domain resource migration support** Not checked yet NEW

25

`fastly-tf-migrate` migrates standalone `fastly_domain` resources.

— Single-line mention with no mechanism or example.

Fastly Terraform Provider (beta) 0.2.11…

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

PortSwigger Burp Suite

Feedback ⓘ

Professional / Community 2026.11.3 (2026-11-25) BLOG ↗ RANK

Burp Suite is a we enable the world to secure the web. Burp Suite, the Web Security Academy, and world-leading research from PortSwigger â the AppSec communityâs home.

> Burp Suite 2026.11.3 adds a new Academy tab for accessing Web Security Academy labs directly inside the tool, plus easier project switching and restarting.

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

01 **Academy tab for Web Security Academy labs** Not checked yet NEW

50

A new Academy tab in Burp Suite's top navigation bar lets users browse and launch Web Security Academy labs directly inside the tool, without leaving the application during a pen test session.

Open Web Security Academy labs without leaving Burp Suite, useful when following along with lab exercises during a pen test session.

> 📍 In Burp Suite, click the Academy tab in the top navigation bar to browse and launch Web Security Academy labs directly.

– Names exact UI path but no deeper mechanism Professional / Community 2026.11.3 (202…

02 **Easier project switching and restart** Not checked yet IMPROVED

20

Users can now switch projects and restart Burp more easily from within the UI.

– Vague improvement with no UI path or mechanism given

Professional / Community 2026.11.3 (202…

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

go-tuf

Feedback ⓘ v2.5.0 NOTES ↗ RANK

Go implementation of The Update Framework (TUF)

> go-tuf v2.5.0 adds post-quantum ML-DSA key support for TUF metadata signing and moves to TUF specification v1.0.37, tightening metadata validation and changing how delegation hash-prefixes and P-384 keys are handled — several of these changes are breaking.

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

01 Post-quantum ML-DSA signing support

Not checked yet NEW

90

go-tuf can now sign TUF metadata using post-quantum ML-DSA keys (`ml-dsa-44/1`, `ml-dsa-65/1`, `ml-dsa-87/1`) via `KeyFromPublicKey` and `Metadata.Sign`, implementing TAP 21.

Sign TUF root metadata with a post-quantum ML-DSA-65 key so your repository can survive quantum-capable adversaries.

go

```
import (
    "github.com/cloudflare/circl/sign/mldsa/mldsa65"
    "github.com/theupdateframework/go-tuf/v2/metadata"
)

// Generate or load an ML-DSA-65 key pair
pub, priv, _ := mldsa65.GenerateKey(nil)

// Derive the TUF Key and add it to the root role
tufKey, _ := metadata.KeyFromPublicKey(pub)
root.Signed.AddKey(tufKey, "root")

// Sign the root metadata
root.Sign(mldsaSigner)
```

— Names exact algorithms and APIs with a runnable code example v2.5.0

02 MultiRepoClient error handling and deterministic refresh

Not checked yet IMPROVED

90

`MultiRepoClient` now exposes `ErrMissingRepoURL`, `ErrUnknownMappingRepo`, and `ErrMissingTrustedRoot` errors and validates `map.json` before initializing any

client. `MultiRepoClient.Refresh` now refreshes all repositories in deterministic order and joins errors from multiple repositories.

Bootstrap a multi-repository TUF client and distinguish between specific initialisation errors (missing URL, unknown mapping repo, or missing trusted root) so your tooling can surface a clear failure reason.

```go
import (
    "errors"
    "github.com/theupdateframework/go-tuf/v2/metadata/multirepo"
)

client, err := multirepo.NewMultiRepoClient(config, fetcher)
if err != nil {
    switch {
    case errors.Is(err, multirepo.ErrMissingRepoURL):
        log.Fatal("map.json references a repo with no URL")
    case errors.Is(err, multirepo.ErrUnknownMappingRepo):
        log.Fatal("map.json maps to an unknown repository")
    case errors.Is(err, multirepo.ErrMissingTrustedRoot):
        log.Fatal("no trusted root found for a mapped
repository")
    }
}
```

— Named error types and method with a runnable example `v2.5.0`

---

03 **TUF spec v1.0.37 compliance and stricter metadata validation**

`Not checked yet` 90

`BREAKING`

go-tuf now implements TUF specification v1.0.37, bumping `SPECIFICATION_VERSION` to `1.0.37`; target lookup now re-visits and verifies shared delegated roles reached via multiple paths. `FromBytes` and `UnmarshalJSON` now reject malformed or non-`1.x` `spec_version` values, `version < 1`, missing required top-level roles, duplicate delegated role names, roles specifying both `paths` and `path_hash_prefixes`, and `null` map entries, with parse errors classified as `metadata.ErrDeserialization`. `path_hash_prefixes` now matches hex-encoded SHA-256 digests instead of base64, and delegation path patterns use OS-independent POSIX `path.Match`, surfacing `path.ErrBadPattern` on invalid patterns; previously cached local files failing these checks will trigger a re-fetch.

— Full before/after mechanism with every rejected case named `v2.5.0`

---

04 **P-384 key ID canonicalization change** `Not checked yet`

`BREAKING`

85

`KeyFromPublicKey` now assigns `ecdsa-sha2-nistp384` to P-384 keys, changing their canonical key ID and requiring SHA-384 signatures, and rejects curves other than P-256 and P-384. Repositories rotating a P-384 root key must include a SHA-256 signature under the old key ID alongside the new signature so clients on the previous root can verify the transition.

— Exact field names and a migration note for root rotation v2.5.0

---

05 **Sign now verifies output and requires RSA-PSS** Not checked yet

75

BREAKING

`Sign` now verifies the signature it produces before storing it and replaces duplicate signatures in place; RSA PKCS #1 v1.5 signers (such as Sigstore's default `signature.LoadSigner` on RSA keys) are rejected for `rsassa-pss-sha256` keys — use `signature.LoadRSAPSSSigner` instead.

— Names the rejected signer and the replacement API v2.5.0

THINNER COVERAGE BELOW

06 **Fetcher no longer mutates http.DefaultClient** Not checked yet

IMPROVED

45

`DefaultFetcher.SetTransport` and `NewFetcherWithRoundTripper` no longer mutate `http.DefaultClient`.

— Named functions but no scope of prior impact described v2.5.0

---

07 **AddKey rejects unconfigured delegated role keys** Not checked yet

IMPROVED

35

`TargetsType.AddKey` now rejects keys for unconfigured delegated roles.

— Single-line change with no further mechanism given v2.5.0

---

08 **Go 1.27 minimum version requirement** Not checked yet

BREAKING

35

Go 1.27 is now the minimum required version, up from Go 1.25.0.

— Bare version bump with no further detail v2.5.0

└──▷ BREAKING ON UPGRADE

! Go 1.27 is now the minimum required version (up from Go 1.25.0).

! `KeyFromPublicKey` now assigns `ecdsa-sha2-nistp384` to P-384 keys, changing their canonical key ID and requiring SHA-384 signatures; repositories rotating a P-384 root key must include a SHA-256 signature under the old key ID alongside the new signature so clients on the previous root can verify the transition.

! `Sign` now rejects RSA signers using PKCS #1 v1.5 (such as Sigstore's default `signature.LoadSigner` on RSA keys) for `rsassa-pss-sha256` keys — use `signature.LoadRSAPSSSigner` instead.

! `FromBytes` and `UnmarshalJSON` now reject previously accepted malformed metadata (non-`1.x` `spec_version`, `version < 1`, missing required roles, duplicate delegated role names, roles with both `paths` and `path_hash_prefixes`, `null` map entries); previously cached local files failing these checks will trigger a re-fetch.

! `path_hash_prefixes` now matches hex-encoded SHA-256 digests instead of base64, changing which delegations match for any repository using hash-prefix delegations.

WAS THIS USEFUL?  

Cloudsmith

Feedback ⓘ

`Hex upstreams are now generally available (2026-11-25)` BLOG ↗

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

Hex upstreams are now self-service: no support request needed to proxy Elixir and Erlang packages from hex.pm through a Cloudsmith repository.

NEW SUPPORTED PLATFORM Hex upstream support (general availability): hex.pm, Elixir, Erlang

---

WAS THIS USEFUL?  

JFrog

Feedback ⓘ

JFrog and Pluto Partner Together on AI Supply Chain Security (2026-11-24)

BLOG ↗ RANK

JFrog software supply chain solutions provide an end-to-end pipeline to control your binaries from build to production. Power your software updates to the edge.

> JFrog partnered with Pluto Security to extend its policy controls from Artifactory, Curation, Xray, and AI Security into AI agent runtimes and developer endpoints.

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

01 **Pluto Security integration for AI agent policy enforcement**

Not checked yet NEW 64

A new integration with Pluto Security extends JFrog's approved lists from Artifactory, Curation, Xray, and AI Security to AI agent runtimes and developer machines where Pluto is deployed, covering packages, models, MCP servers, and skills. Pluto intercepts and automatically enforces JFrog policy at the endpoint for every install, publish, and MCP server connection attempt, blocking pulls from unapproved public registries and external publish targets without manual approval.

.
.
.

— Describes mechanism and scope but no config keys or commands given

JFrog and Pluto Partner Together on AI …

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Reverse Engineering

Finite State Platform

Feedback ⓘ

November 25, 2026 - Dependency warning, CVE project list, and SBOM export (2026-11-25)

BLOG ↗ RANK

Finite State Platform is a firmware security analysis tool that identifies vulnerabilities, software composition, and risks in connected device and IoT firmware at scale.

> Finite State Platform added duplicate-dependency detection for Versions, bulk management controls for large dependency lists, and a tenfold increase to the dependency tree page size.

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

01 **Dependency tree page size raised to 10,000** Not checked yet

IMPROVED 65

The dependency tree page of top-level components can now be as large as 10,000 — the maximum the API accepts — up from 1,000.

— Clear before/after numbers but no config key or command

November 25, 2026 - Dependency warning,…

02 **Edit and Delete menu on large dependency lists** Not checked yet

NEW 60

Every Project Dependencies row on a Version with more than 500 dependencies now has an Edit and Delete menu so older rows can be managed.

— Names the threshold and control but not exact UI location

November 25, 2026 - Dependency warning,…

THINNER COVERAGE BELOW

03 **Duplicate child Project warning on Versions** Not checked yet NEW

55

Versions with more than one version of the same child Project now display a warning that names the child Projects with the most versions and links directly to Project Dependencies for review.

— UI behaviour described but no exact navigation path given

November 25, 2026 - Dependency warning,…

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

Netcap

Feedback ⓘ v0.16.16 NOTES ↗ CODE ↗ RANK

Netcap is a framework for secure and scalable analysis of network traffic, converting pcap files into typed audit records for efficient processing.

> Netcap v0.16.16 restores the WebUI dashboard, adding capture-scoped data views, aggregate traffic totals, and consistency fixes for paginated alert groups.

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

01 **WebUI dashboard restoration and capture scoping** Not checked yet

IMPROVED 57

The WebUI's All PCAPs traffic overview now shows aggregate totals and charts on first visit, with direct capture links retaining their selection. Data pages (Hosts, Devices, Connections, HTTP, Services, and other inventories) now load records scoped to the selected capture with visitor isolation, the Audit Records view keeps a single capture selector, the Alerts and Files pages drop page-level diagnostics while retaining detailed evidence, and grouped alert pagination tokens are now invalidated when an alert outside the capped preview changes to keep paged alert groups consistent.

— Describes multiple UI behaviours but no concrete commands or config v0.16.16

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Qualys TotalCloud

Feedback ⓘ changelog · Nov 26, 2026

BLOG ↗ RANK

Qualys TotalCloud is a cloud-native security platform that provides continuous visibility, risk assessment, and compliance management across multi-cloud environments.

> Qualys TotalCloud launches TotalAI, a new module that red-teams AI models, scans MCP servers and CI/CD pipelines for exposed secrets, builds an AI service inventory, and adds AI-aware identity and network monitoring.

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

01 **AI model red-teaming in TotalAI** Not checked yet NEW 80

TotalAI can red-team any model with a chat completion endpoint — including foreign models — against 300+ attack scenarios mapped to OWASP, MITRE ATLAS, and the EU AI Act, including 21 sensitive information disclosure checks.

— Names frameworks and check counts but no exact command 2026-11-26-d8ae8b2a

02 **AI service inventory across cloud estate** Not checked yet NEW 60

TotalAI maps managed AI services, AI software, and GPU usage across cloud connectors, Cloud Agents, Container Security, and a browser plug-in to build an AI inventory without requiring a separate agent.

— Names integration surfaces but no setup steps 2026-11-26-d8ae8b2a

03 **CIEM posture checks for AI identities** Not checked yet NEW 60

TotalCloud CIEM posture checks show what each cloud identity can access and flag excess privileges for AI services such as Amazon Bedrock, SageMaker, and Azure OpenAI.

— Names specific AI services covered, no exact UI path 2026-11-26-d8ae8b2a

THINNER COVERAGE BELOW

04 **Secrets detection across MCP servers and CI/CD** Not checked yet

NEW

55

TotalAI MCP scans catch secrets that agents source context from in MCP servers, while a parallel capability detects exposed secrets in container images, CI/CD pipelines, and code repositories before they reach a model prompt.

— Names surfaces scanned but no interface or command given 2026-11-26-d8ae8b2a

05 **Network correlation for AI endpoint tracking** Not checked yet

NEW

50

TotalAI correlates DNS and outbound TCP events from monitored workloads to track direct connections to AI routers or provider endpoints outside an approved list.

— Explains mechanism but no config or threshold detail 2026-11-26-d8ae8b2a

WAS THIS USEFUL? 👍 👎

Plerion

Feedback ⓘ Azure workload scanning only where it can run:

NOTES ↗

Plerion is a cloud security platform that provides risk-based prioritization and remediation guidance across cloud infrastructure, helping teams identify and fix critical vulnerabilities efficiently.

Plerion's Azure install script now reports every subscription it skipped or could not set up, so operators know exactly which ones are not being scanned.

The Azure install script now skips subscriptions that lack the required resource providers and lists every skipped or failed subscription at the end of the run, leaving nothing to clean up. Not checked yet

UPDATED SUPPORTED PLATFORM Azure workload scanning prerequisite enforcement: Microsoft.Compute, Microsoft.Network

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

Anchore

Feedback ⓘ

Anchore Open-Source: Celebrating 100 Million Downloads (2026-11-19) BLOG ↗

Anchore's software supply chain solutions automate vulnerability scanning, strengthen container security, and support compliance with NIST, FedRAMP & more.

Syft adds SPDX 3.X output and PURL generation as standard; Grype scan results now include event timestamps and NVD SSVC decorations; Grant adds a native Windows build.

Syft now generates PURLs as standard and adds SPDX 3.X output support. Not checked yet

Grype scan results now include new event timestamps and NVD SSVC decorations in vulnerability match data. Not checked yet

Grant adds a native Windows build to its published release set. Not checked yet

NEW VULNERABILITY CHECK Go Vulnerability Database integration with reachability-aware scanning: GoLang ecosystem

NEW SUPPORTED PLATFORM New Linux distro vulnerability providers in Grype: Photon OS, Fedora, Red Hat Hummingbird, Ubuntu ESM, SUSE Linux Enterprise Server

NEW SUPPORTED PLATFORM New software ecosystem cataloging in Syft: Perl/CPAN, macOS .app bundles, OpenWRT packages, GGUF LLM models, .safetensors LLM model formats

NEW SUPPORTED PLATFORM Linux riscv64 build, daemonless Podman, and OCI layout support in Syft: OCI layouts

NEW INTEGRATION CSAF VEX, OpenVEX, and CycloneDX format support in Grype

NEW COMPLIANCE FRAMEWORK Compound license expression support and updated license standards in Grant: compound license expressions

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

Sysdig Secure

Feedback ⓘ Secure SaaS - November 25, 2026

BLOG ↗ RANK

Sysdig Secure is a cloud-native security platform that detects threats, manages vulnerabilities, and ensures compliance across containers, Kubernetes, and cloud infrastructure.

> Sysdig Secure makes Validated Exposure self-service, letting teams turn it on for AWS, GCP, and Azure accounts directly in the UI or via infrastructure-as-code without contacting support.

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

01 **Self-service Validated Exposure enablement** Not checked yet NEW

80

Validated Exposure can now be enabled for individual AWS, GCP, or Azure accounts, or for an entire organization, via `Integrations > Environments` in the account details panel, without contacting Sysdig Support. It can also be enabled during account onboarding via Terraform, CloudFormation, or the `sysdig-onboarding` skill.

Turn on Validated Exposure for a single cloud account from the Sysdig Secure UI without opening a support ticket.

> 📍 In Sysdig Secure, go to Integrations › Environments, open the account details panel for your AWS, GCP, or Azure account, and toggle Validated Exposure on.

— Names exact UI path and onboarding tools; lacks deeper mechanism detail

Secure SaaS - November 25, 2026

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Huntress

Feedback ⓘ Set up SSO setup with fewer manual steps

NOTES ↗ RANK

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

> Huntress streamlined SSO setup in Settings > Access Management by adding metadata XML import and live sign-in validation before saving.

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

01 **Faster SSO setup via metadata import and validation**

Not checked yet IMPROVED 85

In `Settings > Access Management`, admins can now import their identity provider's metadata XML instead of copying configuration values one by one, and use Validate and Save to test SSO sign-in with the identity provider without being logged out. On success the configuration saves automatically; on failure inline error detail is shown.

When onboarding a new identity provider, import its metadata XML to skip manual field-by-field entry and validate the config live before committing it.

> 📍 In Huntress, go to Settings › Access Management, upload your identity provider's metadata XML file, then select Validate and Save to confirm sign-in works before the configuration is applied.

— Names exact UI path and both new controls with behavior.

Set up SSO setup with fewer manual steps

WAS THIS USEFUL? 👍 👎

Qualys EDR

Feedback ⓘ changelog · Nov 26, 2026 BLOG ↗

Qualys EDR is an endpoint detection and response solution that monitors, detects, and responds to advanced threats and malicious activity on endpoints.

NEW DETECTION Known vulnerability and default credential detections for self-hosted AI model servers: Ollama, vLLM, LiteLLM

NEW DETECTION AI Detection and Response (AI-DR) — real-time attack detection on AI assets: Ollama, vLLM, LiteLLM

WAS THIS USEFUL? 👍 👎

Trend Vision One

Feedback ⓘ

Agentless Vulnerability & Threat Detection version 1.668.11191608 (2026-11-20)

BLOG ↗ RANK

Trend Vision One is a unified cybersecurity platform that integrates threat detection, response, and risk management across endpoints, networks, and cloud environments.

> Trend Vision One hardened its Agentless Vulnerability & Threat Detection scanner for AWS ECS and updated Forward Proxy Service certificate handling.

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

01 **Read-only root filesystem for ECS scanner tasks** Not checked yet

IMPROVED 70

Agentless Vulnerability & Threat Detection's Amazon ECS scanner tasks now run with a read-only root filesystem, aligning with the AWS best practice checked by the `ecs-containers-readonly-access` AWS Config rule. This change requires a CloudFormation stack update to take effect.

— Names exact AWS Config rule and required migration step

Agentless Vulnerability & Threat Detect…

THINNER COVERAGE BELOW

02 **Appliance-managed certificate bundle in Forward Proxy**

Not checked yet IMPROVED 30

Forward Proxy Service now uses the appliance-managed certificate bundle to support custom certificates.

— Describes change but no config detail or steps Service Gateway: Forward Proxy Service …

WAS THIS USEFUL? 👍 👎

XFA

Feedback ⓘ Breach alerts for your email domains NOTES ↗ RANK

XFA is a developer tool that enables building fast, interactive forms and data collection interfaces for web applications.

> XFA shipped a self-service My Account portal letting users manage their own sign-in methods, with admin controls to permit or restrict it.

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

01 **Self-service My Account portal** Not checked yet NEW 63

A new My Account portal lets every user view and manage their own sign-in methods — trusted devices, passkeys, security keys, and authenticator app — without involving an admin. An admin toggle in My account settings controls whether self-service changes are allowed; admins can confirm it's enabled and share the My Account URL with users so they can add or remove sign-in methods themselves.

Direct a user to their self-service My Account portal to review or add a passkey without involving an admin.

> 📍 In the XFA admin console, go to My account settings and confirm self-service is enabled, then share the My Account URL with users so they can add or remove sign-in methods themselves.

— Names the portal, managed credential types, and admin toggle location.

My account for every user

NEW INTEGRATION Have I Been Pwned integration for breach alerts

NEW INTEGRATION Proton Pass and Proton VPN for Business integration

NEW INTEGRATION Shared Signals integration with Okta, Google Workspace, and Microsoft Entra ID

NEW DETECTION Spoofing protection — DMARC, SPF, DKIM, DNSSEC record checks

> Breach alerts for your email domains NOTES ↗ LATEST STABLE
>
> XFA adds Breach alerts (beta, Max and Enterprise plans) to flag verified-domain email addresses found in data breaches or infostealer logs, with optional user notification via Risk monitor.
>
> New Breach alerts feature detects when an address at a verified email domain appears in a known data breach or infostealer log, using Have I Been Pwned data, with an option to notify the affected person — available under Risk monitor in the dashboard on Max and Enterprise plans (currently in beta). Not checked yet

Secure Proton Pass and Proton VPN with XFA NOTES ↗ STABLE

XFA now acts as the identity provider for Proton Pass and Proton VPN for Business, enforcing passkey sign-in and device checks before access.

Shared Signals tells your identity provider when a device stops passing

NOTES ↗ STABLE

XFA adds Shared Signals (beta, Enterprise plan) to push near-real-time policy-failure events to identity providers, enabling proactive session termination.

New Shared Signals integration notifies your identity provider within minutes when a device stops passing policy, so the provider can end the device's sessions before the next sign-in. Not checked yet

Spoofing protection for your email domains NOTES ↗ STABLE

XFA adds a beta spoofing protection feature, available on all plans including Free, accessible under Risk monitor in the dashboard.

WAS THIS USEFUL? 👍 👎

◆ SIEM

Databricks

Feedback ⓘ

Genie One desktop app is generally available on Windows (2026-11-26) BLOG ↗

RANK

Databricks is a unified data analytics platform that enables collaborative data engineering, machine learning, and analytics using Apache Spark in the cloud.

> Databricks shipped GA Lakebase Terraform resources for managing Postgres infrastructure as code, a Windows desktop app for Genie One, and a trio of OpenSharing improvements covering directory-based delivery, recipient-specific URLs, and Unity Catalog agent skill sharing, alongside a new storage-tracking system table and a dashboard export fix.

└──▷ **WHAT SHIPPED · 7 FEATURES** most completely described first ? what's the number?

01 **Lakebase Postgres Terraform resources** Not checked yet NEW

90

Eight Lakebase Postgres Terraform resources reached general availability — `databricks_postgres_project`, `databricks_postgres_branch`, `databricks_postgres_endpoint`, `databricks_postgres_database`, `databricks_postgres_role`, `databricks_postgres_catalog`, `databricks_postgres_synced_table`, and `databricks_postgres_snapshot_schedule` — available from Databricks Terraform provider v1.145.0 onward, enabling infrastructure-as-code management of Lakebase Postgres.

Provision a Lakebase Postgres project and a branch in Terraform once the provider is at v1.145.0 or later.

```hcl
terraform {
  required_providers {
    databricks = {
      source  = "databricks/databricks"
      version = ">= 1.145.0"
    }
  }
}

resource "databricks_postgres_project" "main" {
  name = "my-lakebase-project"
}

resource "databricks_postgres_branch" "dev" {
  project_id = databricks_postgres_project.main.id
  name       = "dev"
}
```

— Names all eight resources, provider version, and runnable Terraform example

Lakebase Terraform resources are genera…

02 **Directory-based access for OpenSharing SecureConnect**

Not checked yet NEW 75

A Public Preview feature delivers eligible tables and views via serverless compute instead of per-file pre-signed URLs for better performance, enabled by account admins from the account console Previews page by turning on OpenSharing SecureConnect Directory Based Access .

Account admins enabling the directory-based access preview to improve data delivery performance for OpenSharing SecureConnect recipients.

📍 In the account console, go to Previews and enable OpenSharing SecureConnect Directory Based Access .

— Explains mechanism change and gives exact enablement steps

Directory-based access for OpenSharing …

03 **Table metrics history system table** Not checked yet NEW 70

The `system.storage.table_metrics_history` system table is now generally available for querying daily storage size, attributing storage costs, and finding tables to clean up for Unity Catalog managed tables.

— Names the exact system table to query for storage cost data

Table metrics history system table is n…

04 **Genie One desktop app for Windows** Not checked yet NEW

60

Genie One is now generally available as a Windows desktop app with separate installers for x64 and ARM64 devices, adding window navigation controls and automatic updates on top of the existing web experience.

— Describes platforms and new controls but no install command

Genie One desktop app is generally avai…

THINNER COVERAGE BELOW

05 **Unity Catalog agent skill sharing via OpenSharing and Marketplace**

Not checked yet NEW INTEGRATION NEW

55

Providers can now add Unity Catalog agent skills to OpenSharing shares and Databricks Marketplace listings for Databricks recipients to consume, generally available but requiring the Enhanced Unity AI Gateway preview BETA and, on some accounts, the Agent Skill Sharing preview enabled by an account admin.

— Names required previews but no exact enablement path

Sharing Unity Catalog agent skills with…

06 **Recipient-specific URLs for OpenSharing open recipients**

Not checked yet IMPROVED

50

OpenSharing open recipients now get a recipient-specific URL that embeds the recipient ID in the host name, letting recipients allowlist their own host name instead of a shared regional host name.

— Explains mechanism but no concrete steps to act on it

Recipient-specific URLs for OpenSharing…

07 **Excel export preserves table widget formatting** Not checked yet

IMPROVED

40

Excel (`.xlsx`) files downloaded from a table widget now keep the widget's column display names and column widths.

— Describes the behavior change but it's a minor formatting fix

Dashboard enhancements (2026-11-26)

NEW INTEGRATION Power BI and Tableau Cloud connectors for Genie Code BI imports

Power BI and Tableau Cloud connectors for BI imports (Public Preview) (2026-11-26)

BLOG ↗ LATEST STABLE

Databricks adds Power BI and Tableau Cloud MCP connectors for Genie Code, with `/importBI` checking migrated reports against the live source.

Moonshot AI Kimi K3.1 Pro Fast is now available on Unity Gateway (2026-11-25)

BLOG ↗ STABLE

WAS THIS USEFUL? 👍 👎

Sumo Logic

Feedback ⓘ Usage Attribution (Manage) (2026-11-25)

BLOG ↗ RANK

Sumo Logic is a cloud-native platform that provides real-time log management, security analytics, and observability for applications and infrastructure.

> Sumo Logic introduces a Usage Attribution tab in Account Overview, letting teams break down log ingest volume by data tier, custom tags, and CSV-based ownership mappings, with filter state now persisted across reloads.

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

01 **Usage Attribution tab in Account Overview** Not checked yet NEW

80

A new Usage Attribution tab breaks down ingest volume by data tier and fields such as `_sourceCategory`, collector, and host. Users can add custom tags (e.g., environment, cost center) as breakdown dimensions, which apply only to data ingested after the tag is saved, and can upload a CSV mapping field values to team, owner, and other columns to enable ownership-based usage breakdowns. Filters and the Breakdown by selection are now saved across page reloads on this tab.

Identify which team or cost center is driving the most ingest before a billing review by uploading an ownership CSV and filtering by owner.

📍 In Account Overview, go to the Usage Attribution tab, then under Ownership lookup upload a CSV with columns for field value, team, and owner. Set Breakdown by to your owner column to see per-team ingest volume by data tier.

Slice ingest by deployment environment to spot which environment is consuming the most log volume.

📍 In Account Overview, go to the Usage Attribution tab, select Custom tags, add a tag named environment, then set Breakdown by to environment to see per-environment ingest trends over time.

— Names exact fields and UI path; lacks limits or retention details.

Usage Attribution (Manage) (2026-11-25)

WAS THIS USEFUL? 👍 👎

ClickHouse

Feedback ⓘ announced · Nov 24, 2026 BLOG ↗

ClickHouse® is a real-time analytics database management system

ClickHouse Managed Postgres adds PostgreSQL 19 on day one, with REPACK CONCURRENTLY, WAIT FOR LSN, sequence replication, parallel autovacuum, new system views, and pg_plan_advice.

Use REPACK (CONCURRENTLY) to reclaim table space without blocking production workloads; slot pool size is controlled by `max_repack_replication_slots` and progress is shown in `pg_stat_progress_repack`. Not checked yet

Use WAIT FOR LSN '...' WITH (TIMEOUT '...' , NO_THROW) on read replicas for read-your-writes consistency against asynchronous standbys. Not checked yet

Replicate sequences with `CREATE PUBLICATION ... FOR ALL SEQUENCES` and `ALTER SUBSCRIPTION ... REFRESH SEQUENCES`; exclude tables with FOR ALL TABLES EXCEPT (TABLE ...). Not checked yet

Enable parallel autovacuum index workers via `autovacuum_max_parallel_workers` in Settings and `autovacuum_parallel_workers` per table; monitor ordering with `pg_stat_autovacuum_scores`. Not checked yet

New system views `pg_stat_lock`, `pg_stat_recovery`, and `pg_dsm_registry_allocations` are queryable; EXPLAIN (ANALYZE, IO) and `auto_explain.log_io` now report asynchronous I/O activity. Not checked yet

+2 more

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability & Exposure Management

oxo

Feedback ⓘ v2.25.10 NOTES ↗ RANK

> oxo added a new history-tracking message type for HTTP requests and introduced automatic expiry for persisted set members to bound memory growth.

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

01 HTTP request history tracking message type

Not checked yet NEW

40

Adds the `v3.history.request` message type for tracking HTTP request history, alongside history period fields added to certificate, DNS, and screenshot history messages.

– Names the message type but not its fields or usage v2.25.10

02 Persist mixin set member expiry

Not checked yet IMPROVED

40

Persist mixin set members now automatically expire after 7 days, preventing unbounded memory growth.

– States behaviour and duration but no config control v2.25.9

WAS THIS USEFUL? 👍 👎

faraday-cli

Feedback ⓘ 2.4.0 NOTES ↗ RANK

Faraday-cli is Faraday's Command Line Interface

> Faraday-cli 2.4.0 adds a scope-check bypass flag for authorized pentests and raises its minimum Python and dependency requirements.

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

01 **Scope check bypass for pentests** Not checked yet NEW 88

The `--skip-scope-check` flag on `faraday scan` or `pentest` lets operators bypass the automatic scope check that otherwise blocks out-of-domain targets in self-registered `ext_<domain>` workspaces, for explicitly authorized targets.

Run a FaradAI pentest against a target that falls outside the auto-detected scope of a self-registered workspace, bypassing the scope guard with explicit operator authorization.

```
$ faraday-cli pentest --target https://other-domain.example.com --skip-scope-check
```

— Names exact flag, command and workspace pattern with runnable example 2.4.0

02 **Raised Python and dependency minimums** Not checked yet BREAKING 75

faraday-cli now requires Python >=3.10, pins `cmd2` to 3.x, removes the version ceiling on `validators` and `httpx`, and requires `faraday-plugins` >=1.32.0; installations on Python 3.8 or 3.9, or with older `cmd2`, will no longer work.

— Names exact versions and packages but no migration steps 2.4.0

└──▷ **BREAKING ON UPGRADE**

! Python >=3.10 is now required; installations on Python 3.8 or 3.9 will no longer work.

! `cmd2` is now pinned to 3.x; environments with an older `cmd2` installed must upgrade.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

ConductorOne

Feedback ⓘ changelog · Nov 26, 2026 CHANGELOG ↗

RANK

ConductorOne is an identity governance platform that automates workforce access management and deploys AI agents to streamline access reviews and provisioning.

> ConductorOne shipped a new access-profile review scope for governance campaigns alongside conditional logic and regex validation for request forms.

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

01 **Conditional visibility for request form fields** Not checked yet

NEW 65

Any request form field after the first can get a show only when condition so it appears only when a prior field matches, hiding irrelevant fields from requesters and approvers; this show/hide behaves live in both the web UI and the Slack request modal.

Gate a ticket-link field on a request form so it only appears when a requester checks a specific checkbox, reducing noise for requesters who do not need it.

> 📍 On a request form field for Ticket link, add a show only when condition: show this field only when the 'Has an existing ticket?' checkbox is checked. Save the form — the field will be hidden by default and appear dynamically in both the web UI and the Slack request modal.

– Describes condition mechanism and Slack parity but no config key.

changelog-20261126-bf378f5c

02 **Regex validation on free-text request fields** Not checked yet

NEW 65

Free-text request form fields can be validated against a regular expression with a custom error message, blocking submission until the answer matches; the web UI checks as the requester types while Slack checks on submit.

Enforce a cost-center code format on a request form text field so free-text answers cannot be submitted in an unrecognised format.

> 📍 On a request form text field for Cost center code, add a regular expression (e.g. ^CC-[0-9]{4}$) and set a custom error message such as 'Enter a cost center in the format CC-XXXX'. The web UI checks the value as the requester types; Slack checks on submit.

— Names validation behaviour and UI vs Slack timing difference.

changelog-20261126-bf378f5c

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Clerk Feedback ⓘ

Faster user search, and filters on your metadata (2026-11-25) BLOG ↗ RANK

Clerk is an authentication and user-management platform that provides pre-built UI components, APIs, and SDKs for adding sign-up, sign-in, and identity features to applications.

> Clerk shipped faster, metadata-filterable user search for large applications, plus Native to Web SSO that lets authenticated users move from native apps to web without re-authenticating.

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

01 **Native to Web SSO for iOS, Android, Expo** Not checked yet NEW

41

Clerk adds Native to Web SSO for iOS, Android, and Expo apps, letting authenticated users open a web view or browser without being prompted to sign in again.

— Describes behavior and platforms but no config or API specifics.

Native to Web SSO for iOS, Android, and…

02 **Metadata filters and faster user search** Not checked yet IMPROVED

33

Clerk now lets you filter users by their metadata when searching, alongside improved search performance on large applications.

— Names the capability but no API, flag, or metric detail.

Faster user search, and filters on your…

WAS THIS USEFUL? 👍 👎

Ory

Feedback ⓘ

Ory Network, Ory Hydra, Ory Kratos, Ory Keto v26.4.22 released NOTES ↗ RANK

Discover the latest features, improvements, and updates to Ory.

> Ory shipped a single hardening fix this window: project update and import now reject stale organization IDs.

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

01 **Stale organization ID rejection on project update/import**

Not checked yet IMPROVED 35

Project update and import operations now reject organization IDs that belonged to organizations which have since been removed, preventing silent misconfigurations where a project could be associated with a deleted organization.

– Explains behavior but no API/flag name or reproduction steps given.

Ory Network, Ory Hydra, Ory Kratos, Ory…

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

amneziawg-installer

Feedback ⓘ v6.3.10 NOTES ↗ RANK

1 VPN server on a fresh Ubuntu or Debian VPS with one command. Made for networks that block WireGuard.

> amneziawg-installer adds a `manage block-ru` command for blocking VPN client access to Russian IPv4 addresses, with an exemption list for custom addresses.

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

01 **Block Russian IPv4 addresses via manage block-ru** Not checked yet

NEW 88

New `manage block-ru` command blocks VPN client access to Russian IPv4 addresses using ipset and iptables REJECT. `block-ru on` enables the block, `block-ru off` removes it, `block-ru update` downloads a fresh address list immediately, and running it with no argument shows current state. Custom addresses (e.g. sites behind a foreign CDN) can be exempted by listing them in `/root/awg/block-ru.extra`.

Enable the Russian IPv4 block for all VPN clients on a server where circumvention of Russian-hosted content is required.

```
$ sudo manage block-ru on
```

— Names exact subcommands, mechanism, and config file path. v6.3.10

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

RegScale

Feedback ⓘ CLI 7.3.0 (2026-11-25) BLOG ↗ RANK

RegScale is a continuous compliance automation platform that helps organizations manage security controls, audit evidence, and regulatory requirements in real time.

> RegScale CLI 7.3.0 adds support for TLS-inspecting proxy connections and introduces asset criticality profile management commands.

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

01 **TLS-inspecting proxy support via sslX509Strict** Not checked yet

NEW 80

Set `sslX509Strict` to `false` in the CLI config to relax Python 3.13+ strict certificate checking, allowing connections through TLS-inspecting proxies whose certificates lack an Authority Key Identifier.

Allow the RegScale CLI to connect through a corporate TLS-inspecting proxy that injects certificates without an Authority Key Identifier.

yaml

```yaml
sslX509Strict: false
```

— Names exact config key and mechanism CLI 7.3.0 (2026-11-25)

02 **Asset criticality profile commands** Not checked yet NEW

70

New `asset_criticality` CLI commands let users list available criticality profiles and assign a profile to specific assets, e.g. `regscale asset_criticality list`.

List available asset criticality profiles and then tag a specific asset with one.

```
$ regscale asset_criticality list
```

— Names command but lacks deeper mechanism detail CLI 7.3.0 (2026-11-25)

WAS THIS USEFUL? 👍 👎

AGENT

◆ MCP Servers & Tooling

Runlayer

Feedback ⓘ 6.8.0 (2026-11-25) BLOG ↗ RANK

Runlayer is an MCP gateway that enforces identity-mapped permissions and detects threats across the agents and MCP servers employees use.

> Across 6.7.0 and 6.8.0, Runlayer adds day-one agent memory, tightens AI Watch and skill-scanner security rules, gives self-hosted deployments new migration lock-contention controls and diagnostics, and introduces several Deploy/ `runlayer.yaml` validation changes that break existing configurations.

└──▷ **WHAT SHIPPED · 17 FEATURES** most completely described first ? what's the number?

01 **Terraform skill verification protection** Not checked yet BREAKING 88

Changing a `runlayer_skill` resource's `files` or `name` when `is_verified = true` now fails the apply with 'inconsistent result after apply'; re-run the apply with a manage-skills token to verify the new files. Changing a verified skill's files or name removes its verification — even when an admin makes the change — and, with device sync set to Verified skills, the edited skill stops syncing to devices until an admin verifies it again.

— Exact error, resource, and migration path given 6.7.0 (2026-11-25)

02 **Deploy build.context resolution change** Not checked yet BREAKING 88

`runlayer deploy` now resolves `build.context` against the folder that holds `runlayer.yaml`; projects that set `context: ../..` or point to paths outside that folder (including via symlinks) must move `runlayer.yaml` to the parent folder and update `build.dockerfile` accordingly.

— Exact migration steps and config keys named 6.8.0 (2026-11-25)

03 **AI Watch scanning hardening** Not checked yet IMPROVED 85

AI Watch now treats ambiguous tool calls — where the tool name could match two configured servers — as unidentified on Cline, Hermes, and older Gemini CLI and GitHub Copilot CLI, causing Enforce to block and Protect to scan them. `aiwatch scan --all-users` now skips a plugin whose real location is outside the scanned user's profile, preventing cross-user data exposure for Cursor, Codex, GitHub Copilot CLI, Gemini CLI, and OpenCode plugins, and on Windows now stores per-user log, lock, and state files under the SYSTEM profile at

`C:\Windows\System32\config\systemprofile\.runlayer\profiles\<SID>\logs` instead of the signed-out user's own folder.

Repair an existing global plugin install whose editor-settings file contains a Runlayer API key, then rotate the key if another user may have read it.

```
$ runlayer plugins update --client <client> --global
```

— Names exact command, path, and affected clients `6.8.0 (2026-11-25)`

---

04 **Migration lock-contention tuning and diagnostics** Not checked yet

IMPROVED

83

Self-hosted deployments can now tune database migration lock-contention behaviour via new Terraform inputs `migration_escalated_lock_timeout_ms`, `migration_base_tier_attempts`, and `migration_escalated_tier_attempts`; when a migration attempt times out waiting for a lock, diagnostics now also list the sessions with the oldest open transactions holding table locks.

Override migration lock-contention settings in Terraform when upgrading a busy self-hosted database, then restore the defaults afterwards.

```hcl
migration_escalated_lock_timeout_ms = 120000
migration_base_tier_attempts      = 5
migration_escalated_tier_attempts = 3
```

— Names exact Terraform inputs and diagnostic behaviour `6.8.0 (2026-11-25)` `6.7.0 (2026-11-25)`

---

05 **Day-one memory for Agents workspaces** Not checked yet NEW

83

Agents workspaces gain day-one memory, giving agents context on each newly added or linked teammate from their public Slack or Teams activity. Enable it on self-hosted deployments by adding `agent-memory-v2` and `day-one-memory` to the `FF_ENABLE` environment variable alongside `agents`, and turn it off per workspace in memory settings.

Enable agent memory on a self-hosted Runlayer deployment so workspaces get the Memories page and day-one memory for new teammates.

```env
FF_ENABLE=agents,agent-memory-v2,day-one-memory
```

– Exact env var and flags given with example 6.7.0 (2026-11-25)

06 **Agent run timeouts and retries via run_agent** Not checked yet

NEW

78

`run_agent` now accepts `timeout_minutes` and `on_timeout: "cancel"` to report or cancel handed-off runs at a deadline, plus `retry: {max_attempts}` to retry runs that failed before any tool call on Pi harness targets.

Cap a handed-off agent run at 10 minutes and cancel it automatically if the deadline is reached, with one retry on infrastructure failure before any tool is called.

```
$ runlayer plugins update --client <client> --global
```

– Exact flags named but no full runnable example 6.8.0 (2026-11-25)

07 **Skill scanner file limits and risk rules** Not checked yet NEW

74

Skill files are now rejected when adding, editing, importing, or restoring would exceed the security scanner's per-skill file limit, and an agent import skips any skill already over the limit. Skill scans also rate a skill High when it hides text in invisible Unicode tag characters (plain or base64-encoded, with the finding showing decoded text), and Medium when an AWS access key ID — alone or with its secret — is found, while documentation placeholder keys such as `AKIAXXXXXXXXXXXXXXXX` are ignored.

– Concrete detection rules and example key named 6.8.0 (2026-11-25) 6.7.0 (2026-11-25)

08 **runlayer.yaml YAML anchor and alias validation (BREAKING)**

Not checked yet

73

BREAKING

A `runlayer.yaml` with YAML aliases that expand beyond roughly twice the 32 KB size limit, or with self-referential anchors, is now rejected on validate, create, or update (rewrite those sections as explicit mappings); similarly, an edit to a Deploy deployment whose masked `env` shares a YAML anchor with another section is now refused, and `env` must be written as its own mapping.

– Exact size threshold and remediation given Clear rule and fix but narrow scope 6.8.0 (2026-11-25)

09 **ToolGuard availability banner** Not checked yet NEW

60

Security admins now see a banner in Settings → Security scanners when ToolGuard is unavailable, showing how long it has been down and how many tool calls and listed tools went unscanned in the last 7 days.

– Exact UI path and metrics shown given 6.7.0 (2026-11-25)

THINNER COVERAGE BELOW

10 **Hosted STDIO connector cloning disabled** Not checked yet BREAKING

58

Cloning a hosted STDIO connector now returns an error instead of creating a copy; use Runlayer Deploy, or create a new remote or local STDIO connector instead.

– Clear before/after but limited mechanism detail 6.8.0 (2026-11-25)

11 **Connector sort controls** Not checked yet NEW

55

The Connectors page can now be sorted by Newest, Oldest, Alphabetical, or Popular using a new sort menu next to Filter; the choice persists in the page URL alongside search and filters.

– Names sort options and URL persistence 6.7.0 (2026-11-25)

12 **Connector test-connection diagnostics** Not checked yet IMPROVED

55

Connector test-connection now shows stage outcomes, HTTP status codes, and timings while keeping credential-bearing request and response details private.

– Describes output but no exact invocation path 6.7.0 (2026-11-25)

13 **Session filtering by agent account** Not checked yet NEW

50

The Sessions view can now be filtered by agent account, surfacing every session that used a given credential, with direct navigation to that account's first call in the selected time range.

– Describes behaviour but no exact UI path given 6.8.0 (2026-11-25)

14 **Connector token revocation hardening** Not checked yet IMPROVED

50

Connector token revocation now sends tokens only to the revocation endpoint recorded at connection time, and only when it shares the same host and port as the provider's token endpoint.

– Explains mechanism but nothing a reader configures 6.8.0 (2026-11-25)

15 **Policy name display in Settings** Not checked yet IMPROVED

42

Settings → Policies and a connector's Policies tab now show the name you gave a policy above its summary, so you can find a named policy without opening it.

– Clear UI path but minor cosmetic change 6.7.0 (2026-11-25)

16 **Slack monitor and trigger privacy restriction** Not checked yet

IMPROVED

40

Slack channel monitors and Slack message triggers now restrict private-channel and group-DM messages to flows whose creator has a linked Slack account and remains in that conversation.

— Clear rule but no config surface to act on 6.8.0 (2026-11-25)

17 **Directory sync role conflict enforcement** Not checked yet IMPROVED

30

Role assignments synced from an external directory can no longer combine with manually assigned roles that would violate separation-of-duties rules.

— Thin prose, no mechanism or config surface named 6.8.0 (2026-11-25)

└──▷ **BREAKING ON UPGRADE**

! `runlayer deploy` now resolves `build.context` against the folder that holds `runlayer.yaml`; projects that set `context: ../..` or point to paths outside that folder (including via symlinks) must move `runlayer.yaml` to the parent folder and update `build.dockerfile` accordingly.

! Cloning a hosted STDIO connector now returns an error instead of creating a copy; use Runlayer Deploy, or create a new remote or local STDIO connector instead.

! A `runlayer.yaml` with YAML aliases that expand beyond roughly twice the 32 KB size limit, or with self-referential anchors, is now rejected on validate, create, or update; rewrite those sections as explicit mappings.

! An edit to a Deploy deployment whose masked env shares a YAML anchor with another section is now refused; write `env` as its own mapping.

! Changing a `runlayer_skill` resource's `files` or `name` when `is_verified = true` now fails the Terraform apply with 'inconsistent result after apply'; a re-run with a manage-skills token is required to verify the new files.

! Changing a verified skill's files or name removes its verification — even when an admin makes the change — and, with device sync set to Verified skills, the edited skill stops syncing to devices until an admin verifies it again.

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI Red Teaming & Testing

AI-Infra-Guard

Feedback ⓘ v4.6.12 NOTES ↗

AI-Infra-Guard is a full-stack AI Red Teaming platform securing AI ecosystems via Agent Scan, Skills Scan, MCP scan, AI Infra scan and LLM jailbreak evaluation.

Agent-Scan adds sandboxed `--repo` source scanning with Stage 1 profiling; Skill-Scan now applies baseline-anchored semantic slicing for pure semantic files.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v4.6.12 https://github.com/Tencent/AI-Infra-Guard.git
# already have the repo? check out this version:
$ git checkout v4.6.12
```

Scan agent repositories in a sandboxed environment with Stage 1 profiling by passing `--repo` as a sandboxed source to `aig-agent-scan`. Not checked yet

AI-Infra-Guard's Skill-Scan now applies baseline-anchored semantic slicing when analysing pure semantic skill files. Not checked yet

NEW DETECTION Cross-server tool shadowing detection rule for MCP

NEW DETECTION RefusalLadderJailbreaking multi-turn attack scenario

WAS THIS USEFUL? 👍 👎

◆ Model & Agent Protection

ToolHive

Feedback ⓘ v0.69.1 NOTES ↗ RANK

> ToolHive's v0.69.1 release focuses on identity and token handling, adding per-client access token lifespans, authorization scope processing, and improved audit traceability, alongside a richer data model for MCP tool-calls and finer-grained scan exclusions.

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

01 **Wildcard directory patterns in .thvignore** Not checked yet NEW

55

ToolHive can now match wildcard directory patterns in `.thvignore` to control which paths are excluded from scanning.

– Names exact config file and pattern mechanism v0.69.1

02 **authorization_details claim processing for ID-JAG tokens**

Not checked yet NEW

50

ToolHive processes the `authorization_details` claim from ID-JAG tokens to support fine-grained authorization scopes.

– Names exact claim but no usage steps v0.69.1

03 **Per-client access token lifespan for ID-JAG redemption**

Not checked yet NEW

35

ToolHive now supports configuring a per-client lifespan for access tokens used in ID-JAG redemption, allowing different clients to have different token validity windows.

– Named but mechanism and config surface not detailed v0.69.1

04 **MCP tool-call details type in data model** Not checked yet NEW

35

ToolHive adds an MCP tool-call details type to its data model, enabling richer introspection of individual tool calls.

– Names the data model addition but not its fields or access v0.69.1

05 **Audit trace of token admission on Identity record** Not checked yet

IMPROVED 30

ToolHive now records how a token was admitted on the Identity record, improving audit traceability of authentication events.

— Describes what changed but not how to view it v0.69.1

WAS THIS USEFUL? 👍 👎

Minimal Software Research minimal Feedback ⓘ

release-7b9ec7d4 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 shipped a browser-based GitHub sign-in flow for `min login`, added naming for the QUIC block helper and detach keys for exec sessions, and removed two legacy commands in favor of their replacements.

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

01 **Named QUIC block helper in finalize-install** Not checked yet

IMPROVED 40

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

— Bare one-line mention with no further mechanism release-7b9ec7d4

02 **Detach keys for exec attach sessions** Not checked yet NEW

30

You can now detach from an exec attach session using the detach keys (tracked as T44).

— No key combination or usage detail given release-7b9ec7d4

└──▷ **BREAKING ON UPGRADE**

! The bare `min stop` and `min task run --path` commands are removed; use `min host stop` and `-C <dir>` instead.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

Bugcrowd Researcher Platform

Feedback ⓘ

changelog · Nov 26, 2026 CHANGELOG ↗ RANK

Bugcrowd Researcher Platform is a crowdsourced security marketplace connecting ethical hackers with organizations to discover and report vulnerabilities through bug bounty programs.

> Bugcrowd Researcher Platform introduced a submission limit per researcher account.

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

01 **Account submission limit** Not checked yet NEW 20

Bugcrowd Researcher Platform now enforces an account submission limit per researcher account, capping how many submissions a given account can make.

— No numeric limit, scope, or mechanism given. changelog-20261126-c7c83c74

WAS THIS USEFUL? 👍 👎

GitHub CLI

Feedback ⓘ v2.106.0 NOTES ↗ RANK

GitHub CLI github's official command line tool

> GitHub CLI's `gh auth logout` now revokes the OAuth token and clears saved Git credentials by default, with an opt-out flag for local-only logout.

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

01 **OAuth revocation and credential cleanup on logout** Not checked yet

IMPROVED 70

`gh auth logout` now revokes the OAuth token on GitHub and also removes saved HTTPS credentials for the host from Git credential helpers. The new `--no-revoke` flag preserves the old local-only behaviour, keeping the OAuth token valid — useful when the token is shared with another tool or machine.

Log out while keeping the OAuth token valid on GitHub — useful when the same token is shared with another tool or machine.

```
$ gh auth logout --no-revoke
```

— Names exact command and flag, but limited mechanism detail beyond that. v2.106.0

WAS THIS USEFUL? 👍 👎

OTHER / UNCATEGORIZED

◆ UNCATEGORIZED

vigolium

Feedback ⓘ v0.5.8 NOTES ↗ RANK

Vigolium - High-fidelity vulnerability scanner fusing agentic AI with native speed, modularity, and precision

> Vigolium v0.5.8 adds host-scoped SQLite imports, richer WAF block classification, a gRPC surface audit command, HTTP/2 and WebSocket inspection, incremental scans, and a cluster of breaking changes around state directories, config overlays, and ingest/migration defaults.

└──▷ **WHAT SHIPPED · 13 FEATURES** most completely described first ? what's the number?

01 **gRPC surface audit command** Not checked yet NEW 90

Audit a gRPC server's exposed services and methods with `grpc-surface-audit`, which queries server-reflection (v1, then v1alpha) for `ListServices` and each service's file descriptor; results appear in `metadata.services` with input/output types and streaming flags.

— Command, protocol versions, and output location named v0.5.8

02 **Per-invocation config overlay with --set** Not checked yet BREAKING 90

Overlay any config key for a single invocation with `--set <dotted.key>=<value>` (repeatable, every command) without writing the file; `config get` / `ls` report the source as `set`, and `config env --set` is now `config env --only-set`, so scripts calling the old flag must be updated.

Override the scan intensity for a single run without touching the config file, useful for a quick manual check.

```
$ vigolium scan --set dynamic-assessment.max_module_tier=2 --
events https://staging.example.com
```

— Flag, rename, and example command all given v0.5.8

03 **Host-scoped SQLite import with skip-findings** Not checked yet NEW 85

Merge only one host's records from a SQLite source with `import <vigolium.sqlite> --host <pattern>`, or strip findings entirely with `import --skip-findings`; a non-SQLite source rejects both flags with `source_incompatible`, exit 2.

Merge only one host's findings from a nightly SQLite dump into the current project, skipping records already present.

```
$ vigolium import nightly.sqlite --host api.example.com
```

— Exact command, flags, and error code given v0.5.8

04 **Hand-framed HTTP/2 probing** Not checked yet NEW 85

Send a hand-framed HTTP/2 request with `kit h2-probe` (flags: `--open-stream`, `--chunk-size`) and get back the server's answer or `timed_out` with `elapsed_ms`.

— Runnable command with flags and output fields v0.5.8

05 **Persistent browser session file** Not checked yet NEW 80

Write and reuse browser session cookies and User-Agent across invocations with `--browser-session-file <path>` (mode 0600); the file never carries an Authorization token and is left unwritten when an authenticated session is in use (feature `browser-session-clearance-only`).

— Flag, file mode, and security behaviour specified v0.5.8

06 **WAF block classification with vendor detection** Not checked yet NEW 75

WAF block events now carry `block_kind` (`vendor`, `challenge`, `refused`) and `transport` (`requester`, `discovery`, `spider`), with vendor challenge pages on HTTP 200 or 202 (Cloudflare, AWS WAF, Akamai, Imperva, Sucuri, DataDome, PerimeterX, Vercel) classified as blocks via exact header or template markers.

— Named fields and vendors but no command to invoke v0.5.8

07 **Header parameter mining in param-mine kit** Not checked yet NEW 75

Mine request header names with `kit param-mine --location header` (built-in list via `kit wordlist headers`), scored like parameters; framing, routing and session headers are excluded.

— Command given, exclusions named, no run example v0.5.8

08 **State directory relocation via VIGOLIUM_STATE_DIR** Not checked yet 75

BREAKING

Relocate all vigolium state (config, DB, caches, Chrome for Testing, nuclei templates, etc.) by setting `VIGOLIUM_STATE_DIR`; this replaces the old `VIGOLIUM_HOME`

variable, so existing setups using `VIGOLIUM_HOME` must switch to `VIGOLIUM_STATE_DIR`.

— Env var name and migration note given v0.5.8

09 **Schema DDL export command** Not checked yet NEW 75

Print the SQLite DDL for the current schema with `schema storage --ddl` (or `-j` for `{schema_version, statements}`) without opening a store.

— Command and flags named, no example v0.5.8

10 **Auto-migrate-on-read disabled by default** Not checked yet BREAKING 70

`database.auto_migrate_on_read` now defaults to false; vigolium will refuse to open a store written by an older version unless `VIGOLIUM_AUTO_MIGRATE=1` is set or `database.auto_migrate_on_read=true` is configured.

— Config key, env var, and default change specified v0.5.8

11 **WebSocket frame capture in browser crawl** Not checked yet NEW 65

The browser crawl now records in-scope WebSocket frames — URL, direction, opcode, payload length, and a 4 KiB head — in the new `websocket_frames` table.

— Table and captured fields named, no retrieval command v0.5.8

12 **Incremental scan via --only-new-since** Not checked yet NEW 65

Re-scan only traffic recorded since the last run using `--only-new-since latest`, speeding up CI pipelines by skipping retesting of old records.

Re-scan only traffic recorded since the last run to speed up CI pipelines without retesting old records.

```
$ vigolium scan --only-new-since latest --events
https://example.com
```

— Flag and example given, mechanism lightly described v0.5.8

THINNER COVERAGE BELOW

13 **Ingest no longer fetches responses by default** Not checked yet 50

BREAKING

`ingest` no longer fetches responses by default; pass `--fetch-responses` to restore the previous behaviour.

— Flag named but minimal mechanism explained v0.5.8

└──▷ BREAKING ON UPGRADE

! `VIGOLIUM_HOME` is replaced by `VIGOLIUM_STATE_DIR`; existing setups using `VIGOLIUM_HOME` must switch to `VIGOLIUM_STATE_DIR` (feature `state-dir`).

! `config env --set` is renamed to `config env --only-set`; scripts calling the old flag must be updated (feature `config-overlay`).

! `database.auto_migrate_on_read` now defaults to false; vigolium will refuse to open a store written by an older version unless `VIGOLIUM_AUTO_MIGRATE=1` is set or `database.auto_migrate_on_read=true` is configured (feature `no-migrate-on-read`).

! `ingest` no longer fetches responses by default; pass `--fetch-responses` to restore the previous behaviour (feature `ingest-no-fetch-default`).

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · November 26, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue