THE CYBER TOOLCHAIN

NO. 124

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 29, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 175 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 52 tools

▾ // THE BRIEF HIDE

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

PROTECT

Scan the binaries your package manager never knew about

vim ? help

Sysdig's Registry and Agentless Host scanners now look at standalone binaries, including PHP built from source — the class of artifact that slips past manifest-driven scanning because nothing ever recorded it as a dependency — and risk acceptance extends to those non-package components so you can actually close the findings. Kubescape attaches CISA KEV and EPSS scores to image scan results, so the ranking argument about which CVE to fix first happens against exploitation evidence rather than CVSS alone.

Sysdig Secure · kubescape

PROTECT

Recover a locked Mac and enroll a Windows box without a reusable secret

On-demand FileVault key rotation means a key exposed in a helpdesk ticket or stale escrow record can be invalidated immediately instead of waiting for a reimage; per-device one-time Windows MDM enroll secrets kill the shared enrollment token that, once leaked, lets anything join your tenant. Self-service and hidden config profiles also take routine profile installs off the IT queue.

Fleet

IDENTIFY

Find out what an attacker can reach from outside, without handing over credentials

Aikido's External Network Pentesting takes a list of top-level domains and has AI agents map and attempt exploitation of the perimeter with no code access or credentials — the same starting position a real attacker has, and cheap enough to run between annual engagements. Hacktron scopes Whitebox pentests to specific folders and issues shareable Attestation Letters, so you can prove a review happened to a customer without forwarding raw findings.

Aikido Security · Hacktron

GOVERN

Pin cloud actions to the human or agent that actually made them

RIG's Gatewatch endpoint agent attributes a cloud API call to the person or AI agent driving it and can block a policy violation before it leaves the host — the gap in every CloudTrail investigation where a shared service role tells you what happened but not who. Aembit's MCP Identity

> Gateway adds a network access policy limiting which MCP servers it will reach, bounding where an agent can go rather than trusting its tool list.
>
> RIG Security

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

Dreadnode

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗ RANK

Documentation for the Dreadnode AI security platform — self-hosting guides, platform concepts, SDK reference, and CLI documentation.

> Dreadnode shipped enriched parquet findings exports, automatic retry for hosted inference streams, pinned chat/session support, an expanded network-ops toolchain for Docker sandboxes, and new AI red-teaming attack and scoring options.

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

01 Network-ops toolchain in Docker sandboxes IMPROVED

75

The network-ops capability now installs a full toolchain locally in Docker sandboxes — `nmap`, `smbclient`, `hashcat`, `john`, `impacket`, `certipy-ad`, `bloodyAD`, and `NetExec` — and exposes structured findings (hosts, users, credentials, shares, and weaknesses) viewable in Agent Output after enumeration.

— Names every installed tool and where findings surface changelog-20261029-b080e3d9

02 Automatic retry for dropped inference streams IMPROVED

65

Hosted inference streams that drop on unstable network paths are now retried automatically up to 3 times with exponential backoff (1 s, 2 s, 4 s).

— Precise retry mechanism and timing, but automatic with no user control

changelog-20261029-b080e3d9

03 GCG-family white-box attacks in AI red-teaming NEW

65

The ai-red-teaming capability supports selecting a GCG-family white-box attack from the attack catalog, using a local open-weight model as the surrogate for the assessment.

Run a white-box GCG attack against a local open-weight model as the surrogate for an AI red-teaming assessment.

📍 # supply a local open-weight model as the surrogate in the ai-red-teaming capability # select a GCG-family white-box attack from the attack catalog when configuring the run

— Describes concrete attack setup steps from the example changelog-20261029-b080e3d9

04 **tool_call_attack_landed scorer for agentic red-team runs** NEW

65

Adding `tool_call_attack_landed` to the scorer list in an airt SDK study configuration scores agentic red-team runs for exact tool-call landings instead of relying on a judge model.

Score an agentic red-team run for exact tool-call landings rather than relying on a judge model.

> 📍 # add tool_call_attack_landed to the scorer list in your airt SDK study configuration

— Names the exact scorer and config location to add it changelog-20261029-b080e3d9

THINNER COVERAGE BELOW

05 **Enriched findings parquet exports** NEW

55

Findings can now be exported as parquet files carrying reviewed severity and status, a full audit trail, ASR (attack success rate), compliance tags, adversarial-ML metrics, and project rollups.

— Names fields exported but no endpoint or command given changelog-20261029-b080e3d9

06 **Pin sessions in Chat and Agents** NEW

55

Sessions can be pinned from the menu in the Chat sidebar, in either Chat or Agents › Sessions, so pinned sessions appear at the top of the list.

— Exact UI path given but no deeper mechanism changelog-20261029-b080e3d9

WAS THIS USEFUL? 👍 👎

Hacktron

Feedback ⓘ

Scope your pentest to exactly the folders that matter NOTES ↗ RANK

Hacktron is an AI-powered security code-review platform. Our AI agents review your repositories for exploitable vulnerabilities and surface them as pull-request comments and dashboard findings.

> Hacktron's latest release lets you scope Whitebox pentests to specific folders, adds a Closed status for findings, introduces shareable Attestation Letters, raises Code Review file and seat limits, and ships a batch of admin and UI improvements across People management, GitLab connections, and the Whitebox review flow.

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

01 **Folder-scoped Whitebox pentest scanning** NEW 70

The Whitebox pentest wizard gains a new Scope step with a checkbox file tree, letting you include or exclude specific folders so the pentest scans only the directories that matter instead of the whole repository.

When launching a Whitebox pentest, narrow the scan to only the directories that are in scope — such as a single service directory — instead of scanning the entire repository.

📍 In the Whitebox pentest wizard, advance to the Scope step, uncheck all top-level folders in the checkbox file tree, then check only the folders you want scanned (e.g. `src/auth` and `src/payments`), then continue to launch the scan.

— Clear UI path and example, no config key named Scope your pentest to exactly the folde…

02 **Attestation Letters page** NEW 70

A new Attestation Letters page lists Hacktron-issued attestation letters, each with a unique shareable link and a PDF download that auditors can view without logging in.

Share a compliance attestation letter with a customer or auditor who does not have a Hacktron account.

📍 Go to your organization's Attestation Letters page, copy the unique shareable link next to the relevant letter, and send it to the recipient — they can view or download the PDF without logging in.

— Example gives full share workflow, no API detail

Scope your pentest to exactly the folde…

03 **Higher Code Review file and seat limits** IMPROVED 70

Pull requests with up to `500` changed files are now accepted for Code Review, up from `200`, and OSS organizations now get `50` free PR reviews per month, up from the previous limit.

— Exact numeric limits named, no config surface Scope your pentest to exactly the folde…

04 **Org-level toggle for automated review comments** NEW

60

Organization admins can turn off automated code review comments for the whole organization from Settings.

Stop Hacktron from posting automated code review comments on every pull request across the whole organization.

> 📍 In Hacktron, go to Settings, find the automated code review comments control, and turn it off at the org level.

— Clear Settings navigation given in example Scope your pentest to exactly the folde…

05 **Structured summary panel for Whitebox review step** IMPROVED

60

The final Whitebox review step is rebuilt as a structured summary panel with Source, Target, Access, and Context sections, each with an Edit button and visible verification status.

— Names sections but lacks deeper mechanism Scope your pentest to exactly the folde…

THINNER COVERAGE BELOW

06 **Closed status for findings** NEW

55

Findings can now be marked Closed directly from the finding's status menu, via keyboard shortcut, or through the command palette — the same surfaces used to set False Positive.

— Names access points but lacks further mechanism

Scope your pentest to exactly the folde…

07 **Members and Invitations tabs in People page** IMPROVED

50

The People page now splits into a Members tab and an Invitations tab, and revoked invitations are listed with a Delete option instead of disappearing.

— UI change described without deeper mechanism Scope your pentest to exactly the folde…

08 **Partial GitLab installation setup** IMPROVED

50

Connecting a GitLab installation no longer requires completing every step before saving — partial setups can be saved, and the connection page shows only the actions available at your current access level.

— Describes behavior change without exact steps Scope your pentest to exactly the folde…

09 **Billable seat disclosures for bot PR authors** IMPROVED 45

Tooltips and prompts at every auto-assignment opt-in point now disclose that bot PR authors take billable seats, and the excluded-authors filter note clarifies that excluded authors never consume a seat.

— Explains behavior but no exact UI path Scope your pentest to exactly the folde…

10 **Enable-all button in trial activation modal** NEW 40

The trial activation modal now has an enable-all button to turn on PR reviews for every connected repository in one step.

— Brief UI feature with minimal detail Scope your pentest to exactly the folde…

WAS THIS USEFUL?  

◆ Hacking Hardware

Hak5 WiFi Pineapple Pager

Feedback ⓘ 2.0.0-stable

NOTES ↗ RANK

A pocket sized WiFi Pineapple built for those on the go.

> WiFi Pineapple Pager 2.0.0 adds Bluetooth/BLE scanning via a new blue5 scanner, native GPS with gpsd configuration, a rebuilt Virtual Pager interface, an offline WiGLE mapping page, and a files browser for managing loot and payloads.

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

01 BLE and Classic Bluetooth scanning with blue5 NEW

95

A new `blue5` scanner provides a live results list, device identification from built-in company and service databases, an events-per-second dashboard with audio, and logging to WiGLE and a SQLite `blue5.db` database tracking up to 25,000 devices in RAM. The `blue5ctl fetch -r` command strips BLE random-address churn so only stable, identifiable devices appear in results.

Strip BLE random-address churn from Bluetooth recon output so only stable, identifiable devices appear in results.

```
$ blue5ctl fetch -r
```

— Names database, limit, and a runnable command 2.0.0-stable

02 Client Access for SSH and Virtual Pager over Client Mode NEW

80

A new Client Access setting under `Settings > System > Virtual Pager` (off by default) enables SSH and Virtual Pager access over a Client Mode network such as a phone hotspot.

Allow a phone hotspot to reach the Virtual Pager and SSH while keeping PineAP APs blocked, useful for field access without a dedicated management device.

> 📍 In the Virtual Pager, go to Settings › System, scroll to Virtual Pager, and enable Client Access.

— Exact UI path and toggle, with usage steps 2.0.0-stable

03 **JSON output for _pineap CLI commands** NEW 78

The `_pineap` CLI commands `INTERFACE LIST` and `SSIDPOOL LIST` now support `format=json` or `format=mjson` for machine-readable output.

Get machine-readable JSON from the PineAP SSID pool for piping into a parsing script.

```
$ _pineap SSIDPOOL LIST format=json
```

— Exact commands and flags with runnable example 2.0.0-stable

04 **Files browser for loot, payloads, and USB storage** NEW 78

The new Files page under `Manage Data > Files` lets users browse, preview, edit, upload, rename, move, delete, and download loot, payloads, `/mmc/root`, and a mounted USB drive, with drag-and-drop upload and whole-folder zip downloads.

— Names exact paths but no runnable example 2.0.0-stable

05 **Native GPS support and gpsd configuration** NEW 75

Native GPS is now built into PineAP and enabled by default on new installs and upgrades, with plugging in a GPS device auto-configuring it. `gpsd` settings — service toggle, serial device, baud rate, and restart — can be configured from the new `Settings > GPS > Advanced` page or via the `hak5-commands` GPS commands.

— Names config page and commands but no example 2.0.0-stable

06 **Rebuilt Virtual Pager interface** IMPROVED 75

The Virtual Pager now scales to any screen size with large touch buttons, keyboard shortcuts (press `?` to list them), a pin-to-every-page shell (press), and side-by-side or stacked Pager and shell panes that can be minimized, maximized, or opened in a new window.

— Names shortcuts and behavior, no config surface 2.0.0-stable

07 **All radios recon dashboard** NEW 73

The Recon page now shows an All radios pane with Wi-Fi and Bluetooth totals, a two-minute packets-and-events graph, breakdowns by encryption, band, channel, and Bluetooth device type, and live searchable, filterable, sortable device tables including AP client lists.

— Detailed dashboard contents, UI-only access 2.0.0-stable

08 **Offline WiGLE map on new WiGLE Logs page** NEW 71

The new `WiGLE Logs` page displays WiGLE logs on an offline map using saved OpenStreetMap, OpenTopoMap, or other tile sets (capped at 500 MB), alongside a

searchable device list and a devices-over-time chart.

— Names page and tile cap, UI navigation only `2.0.0-stable`

THINNER COVERAGE BELOW

09 **Built-in help pages across settings menus** NEW 50

Every settings menu — Display, General, Network, Ringtone, System, Bluetooth, PineAP, Filters, and GPS — now has a built-in help page accessible by pressing right on any item.

— Simple UI addition, thinly described `2.0.0-stable`

WAS THIS USEFUL? 👍 👎

ESP32 Marauder

Feedback ⓘ v1.20.0 NOTES ↗ RANK

A suite of WiFi/Bluetooth offensive and defensive tools for the ESP32.

> ESP32 Marauder v1.20.0 adds guided per-AP WiFi attack profiles, surfaces FCC module IDs with station AP selection, and extends the Censor setting plus detection reliability for Remote ID scanning.

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

01 **Guided per-AP WiFi attack profiles** NEW 60

Adds guided per-AP WiFi attack profiles that walk the user through targeted attacks against a selected access point, rather than broad channel-wide attacks. On the device this is accessed via WiFi > Attacks by selecting a scanned access point and then choosing an attack profile from the guided per-AP menu.

Run a targeted WiFi attack against a specific AP using the new guided per-AP attack profiles instead of broad channel attacks.

> 📍 On the device, go to WiFi › Attacks, select a scanned access point from the list, then choose an attack profile from the guided per-AP menu.

– Describes mechanism and gives exact UI navigation steps v1.20.0

THINNER COVERAGE BELOW

02 **Remote ID detection: Censor masking and reliability fixes**

IMPROVED 45

Applies the existing Censor setting to Remote ID identifiers, masking operator and drone identity data during scans. Remote ID detection also gains improved compatibility and scan timing.

– Names the setting but no steps or scope of timing fix v1.20.0

03 **FCC module ID display and station AP selection** NEW

35

Adds display of FCC module IDs to identify regulatory module details, and adds station AP selection to choose a target access point.

– Named additions but no usage path or mechanism given v1.20.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

Mend.io Mend SAST

Feedback ⓘ changelog · Oct 29, 2026

CHANGELOG ↗ RANK

Mend SAST is a static application security testing service that scans source code for vulnerabilities and helps teams prioritize remediation.

> Mend SAST introduces AI-based project risk factors to help teams prioritize which applications and projects to remediate first.

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

01 **AI-based project risk factors** NEW 69

Mend SAST adds a risk factors column to the Applications and Projects lists, filterable by group or individual risk factor, to help prioritize remediation across projects. An evidence page lists the code signals behind each risk factor classification, grouped by risk factor and file, and a risk factors widget appears on the project summary page for at-a-glance visibility. The capability is enabled from organization administration, requires AI consent, is off by default, and when enabled shares code snippets and project details with Mend's AI model to produce classifications.

— Explains mechanism and UI locations but no API/flag names changelog-20261029-64bd0cb5

WAS THIS USEFUL? 👍 👎

Aikido Security

Feedback ⓘ

🚀External Network Pentesting: test your perimeter before someone else does

NOTES ↗ RANK

Aikido Security is a developer-focused application security platform that scans code, dependencies, containers, and cloud infrastructure to detect and help fix vulnerabilities.

> Aikido Security launches External Network Pentesting, where AI agents autonomously map and attempt to exploit an organization's external perimeter from a list of top-level domains, with no code access or credentials required.

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

01 **External Network Pentesting with AI agents** NEW 85

AI agents discover subdomains, open ports, and services from a list of top-level domains, then attempt exploitation using known CVEs, misconfigurations, and exposed secrets, chaining findings across hosts to pivot and produce a full attack-path report from entry point to impact. A scoping agent checks ownership of each subdomain and restricts testing to owned portions, routing all agent traffic through a proxy that blocks out-of-scope connections; the Agents tab shows each agent's live thinking, tools in use, and findings. Tests can run in Continuous mode so newly discovered subdomains are tested shortly after going live, with intensity controlled via a maximum requests-per-second per target and optional restriction to inside or outside business hours. The resulting report is auditor-ready, formatted like Aikido's existing web app and mobile pentest reports, and covers the attack surface up to the login page.

Start an external network pentest against your perimeter by supplying your top-level domains through the Aikido console.

> 📍 1. In the Aikido console, navigate to Pentesting › External Network Pentesting. 2. Add one or more top-level domains to scope. 3. Review the discovered subdomains, IP addresses, open ports and services; remove anything to keep out of scope. 4. Set your maximum requests per second per target and optionally restrict testing to inside or outside business hours. 5. Click Start Pentest — the quoted credit cost is shown before anything runs.

Enable continuous mode so newly exposed subdomains are automatically tested shortly after they go live, without manually kicking off a new pentest.

> 📍 1. In the Aikido console, open your External Network Pentest configuration. 2. Under Run mode, select Continuous. 3. Confirm the yearly credit price (based on assets found in your first pentest) and save.

— Detailed mechanism, scope controls and UI path, but no API/CLI surface named.

🚀External Network Pentesting: test you…

WAS THIS USEFUL? 👍 👎

psalm-plugin-laravel

Feedback ⓘ v4.18.0 NOTES ↗

Security-focused Laravel static analyser

psalm-plugin-laravel adds opt-in Blade template analysis, a `blade:annotate` command, per-run `--plugin-option` overrides, and Eloquent type narrowing improvements.

└──▷ **GET THIS VERSION** ▾

```
$ git clone --branch v4.18.0 https://github.com/psalm/psalm-plugin-laravel.git
# already have the repo? check out this version:
$ git checkout v4.18.0
```

UPDATED DETECTION Enable Blade template analysis with `<blade />` in `psalm.xml` or `--blade` on the command line; reports broken references, wrong types, and `TaintedHtml` on unescaped `{!! !!}` output at the template's own file and line.

Run `vendor/bin/psalm-laravel blade:annotate` to read view() calls and write matching `@var` declarations into templates; use `--dry-run` to preview the diff without writing.

Override any plugin setting for a single run with `psalm-laravel analyze --plugin-option=KEY=VALUE` (for example, `--plugin-option=experimental=true`); the command line wins over `psalm.xml`.

NEW DETECTION Three experimental view-data checks — `MissingViewData`, `InvalidViewData`, and `UnusedViewData` — compare view(), Mailable, `MailMessage`, and `@includeIsolated` call sites with template declarations; enable as errors with `<experimental value="true" />`.

Roots Laravel convention entry points — `__invoke`, middleware handle()/terminate(), queued job handle()/failed() — in Psalm 7 dead-code detection, removing `UnusedMethod` / `UnusedProperty` cascades behind invokable controllers, middleware, and jobs.

+4 more

UPDATED DETECTION laravel/ai 1.x LLM prompt sink and response source support

UPDATED DETECTION json_encode with JSON_HEX_* flags and Blade @json treated as HTML/quote escape

└──▷ **BREAKING ON UPGRADE**

- ! Minimum Laravel version is now 12.27+ or 13.20+ (was 12.14+ or 13.3+), enforced as a `conflict` on `laravel/framework`.
- ! Minimum Psalm version is now 7.0.0-rc16+.
- ! The `illuminate/*` packages and `orchestra/testbench-core` are no longer required by the plugin; analyzing a Laravel package without `bootstrap/app.php` now requires `orchestra/testbench` in dev dependencies.
- ! Facades registered via config('app.aliases') and `AliasLoader` now use class_alias() instead of an `extends` stub; classes that only the old stubs extended may now report `ClassMustBeFinal`.
- ! `laravel/ai` 0.x LLM prompt sinks and response sources are no longer covered; only 1.x is supported.

WAS THIS USEFUL?  

GitHub Feedback ⓘ

Route and orchestrate models with GitHub Copilot Fusion (2026-10-28) BLOG ↗

RANK

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

> GitHub's Universe releases bundle Copilot Fusion's multi-model routing (now extending to on-device local models), a new Agent Host that keeps Copilot sessions alive and in sync across VS Code, mobile, Slack and Teams via an open Agent Host Protocol, and generally-available Agentic Workflows with built-in sandboxing and threat detection. Alongside these, GitHub Enterprise now bundles Copilot access by default, Copilot Memory reached GA, Dreaming and shared Automations entered preview, and Copilot chat gained a dedicated security extension and native image generation.

└──▷ **WHAT SHIPPED · 16 FEATURES** most completely described first ? what's the number?

01 **Security extension for the Copilot app** NEW 95

Install the extension with `copilot plugin install github-security@awesome-copilot` in the terminal, or search `github-security` in the Copilot app's Customize panel and click Install. Run `/security-review` on local changes to catch new issues before opening a pull request, with the extension flagging when code has changed since the last review; you can also ask Copilot about alerts in chat using the extension's tools, governed by existing tool permission settings. Public preview on github.com and GitHub Enterprise Cloud with data residency; GitHub Enterprise Server is not supported.

Install the GitHub security extension from the terminal so you can immediately browse code scanning alerts in the Copilot app.

```
$ copilot plugin install github-security@awesome-copilot
```

Scan your uncommitted changes for new issues before opening a pull request, without waiting for CI to run code scanning.

```
$ /security-review
```

— Exact install command, slash command, and platform scope given.

Security extension for the GitHub Copil…

02 Agent Host for cross-surface session continuity NEW

93

The new Agent Host isolates Copilot sessions from individual VS Code windows, powering session continuity across VS Code, the Copilot app, GitHub Mobile, github.com, Copilot CLI, Slack, and Microsoft Teams DMs; sessions stay alive after closing a VS Code window or project folder, and extend to remote machines via VS Code's Remote SSH and dev tunnels from the Agents window so agents keep running after disconnect. Start an agent on your dev machine and control it from GitHub Mobile with `code agent host --github-environment` run from your project folder. An open Agent Host Protocol (AHP) lets you build custom clients that share live sessions with VS Code, with client libraries for TypeScript, Rust, Go, Kotlin, and Swift available via `code agent host`. Switching between the editor and the Agents window keeps both in sync with the same live session.

Start a remote agent host so you can control a long-running coding task from your phone or another device while your development machine keeps working.

```
$ code agent host --github-environment
```

— Exact command and protocol named with concrete surfaces listed.

GitHub Copilot in VS Code, Universe rel…

03 GitHub Agentic Workflows generally available IMPROVED

93

GitHub Agentic Workflows lets you define automation in natural language Markdown files that compile to standard Actions YAML and run inside GitHub Actions with existing runner groups and policies, now generally available. Workflows can run on self-hosted Actions Runner Controller runners with Docker-in-Docker support; a model router automatically selects models per workflow optimizing for task type and difficulty, and you can also pick model providers per workflow from a refreshed model inventory. Agents run with read-only permissions by default, execute inside a sandboxed container behind the Agent Workflow Firewall, and have all proposed changes scanned by a dedicated threat detection job before being applied. Use `gh aw forecast` (no longer experimental) for AI credit spend projections including threat detection credits and monthly ranges, and `gh aw add-wizard` to add new workflow templates to a repository.

Check projected AI credit spend, including threat detection costs, before committing to a new agentic workflow rollout.

```
$ gh aw forecast
```

Bootstrap a new agentic workflow from a prebuilt template — such as triage or dependency management — without writing Actions YAML by hand.

```
$ gh aw add-wizard
```

— Exact CLI commands and security mechanisms named.

GitHub Agentic Workflows generally avai…

04 **Shared Copilot Automations for teams** NEW 91

Create shared automations by choosing `Shared` under Type when creating an automation on github.com, the Copilot app, or VS Code, making the workflow visible to all readers and editable by anyone with write access. Shared automations are billed to the organization or user owning the repository rather than the creator, attribute actions to Copilot instead of an individual, persist if the creator leaves the team, and keep a change history of tool/trigger/prompt evolution. Organization admins must enable the 'Allow use of Copilot cloud agent billed to the organization' policy for shared automations to run in org-owned repos. Available on Copilot Pro, Pro+, Max, Business, and Enterprise plans.

Let an org admin gate shared automations to prevent unintended AI credit usage against the organization budget.

> 📍 In your organization settings, go to Copilot › Policies and enable 'Allow use of Copilot cloud agent billed to the organization'.

Create a team-owned automation — for example, to automatically investigate production incidents — so it survives individual team members leaving.

> 📍 On github.com, open a repository where you have write access, navigate to Copilot Automations › New automation, set triggers and tools, then under Type select `Shared` before saving.

— Exact policy name and creation steps given. Build shared workflows for your team wi…

05 **Copilot Fusion multi-model routing and orchestration** NEW 90

Copilot Fusion automatically routes and orchestrates models across Single (one model), Cascade (draft-then-escalate), and Critique (draft-review-revise) workflows, selectable from the model picker without manual switching. Choose an effort level — Fusion Standard, Fusion High, or Fusion Max — to control whether Fusion favors versatile, capable, or most-capable models; enterprise admins can set each model's effective policy state per-Fusion via enterprise/organization model policies, set Fusion as the enterprise default via Enterprise managed settings, and paid-plan users get a 30% cost

discount for a limited time. Fusion now also routes between on-device and cloud models: enable `chat.copilot.localModel.enabled` in VS Code and select Standard in Fusion, configure `MAI Code 1.1 Flash` or `Qwen3.8 Flash Next` via a local OpenAI-compatible server for Copilot CLI, download `MAI Code 1.1 Flash` via the Windows ML provider under Settings > Model providers plus Settings > Experiments > Local model auto routing in the Copilot app, or run `/model` in Copilot CLI with experimental mode enabled on Windows.

When you want Copilot to handle model selection automatically for a demanding refactor or architecture task without manually switching models.

> 📍 Open the model picker in Visual Studio Code or JetBrains, select `Copilot Fusion`, then choose `Fusion Max` as the effort level to apply the most capable models to complex reasoning tasks.

Enable local model routing in VS Code so Copilot Fusion can automatically pick between your on-device model and cloud models without manual switching.

```yaml
chat.copilot.localModel.enabled: true
```

— Names modes, effort levels, config key and model names across two releases.

Route and orchestrate models with GitHu… | GitHub Copilot Fusion now supports sele…

---

06 **Copilot Dreaming public preview** NEW 88

Copilot Dreaming lets Copilot reflect on past sessions to update personal memories, propose changes to repository skills and custom instruction files via pull requests, and turn recurring accepted code-review feedback into standing guidance. It runs three dream types — personal memory curation, repository customization, and code review customization — and is opted into via Copilot settings (individuals) or Copilot policies (organizations and enterprises), e.g. Organization Settings > Copilot > Policies > `Dreaming`.

Enable Copilot Dreaming for your organization so agents continuously refine repository memories and propose instruction updates via pull requests.

> 📍 In GitHub, go to Organization Settings › Copilot › Policies, then enable `Dreaming` to allow agents to update memories and propose skill and custom instruction file changes in pull requests.

— Three dream types and opt-in path named; no API exposed.

GitHub intelligence puts your code, con…

07 **Computer use for desktop app automation** NEW 86

Copilot can now interact with desktop apps — reading content, clicking controls, entering text, navigating UI — including apps with no API, CLI, or MCP integration. In the Copilot app (public preview on macOS and Windows), enable it via Settings > Computer Use > `Enable Computer Use`, granting Accessibility and Screen Recording permissions on macOS. In VS Code, enable `chat.agentHost.computerUse.enabled`, restart VS Code, then run `/computer on` in a Copilot session.

Enable Copilot to control desktop apps (such as expense-report workflows) on a managed macOS machine without requiring an API or MCP integration.

> 📍 In the GitHub Copilot app, go to Settings › Computer Use and turn on `Enable Computer Use`. When prompted by macOS, grant Accessibility and Screen Recording permissions.

Let Copilot interact with desktop apps — filling forms, clicking UI controls — by enabling computer use in VS Code settings and activating it in the current session.

```
$ # 1. In VS Code Settings, enable
chat.agentHost.computerUse.enabled and restart VS Code
# 2. In a Copilot session panel, run:
/computer on
```

— Exact settings and commands given for both client surfaces.

GitHub Copilot app, Universe releases (… | GitHub Copilot in VS Code, Universe rel…

08 Image generation and editing in Copilot chat NEW 83

Generate and edit images using natural language in any Copilot chat session in VS Code, the Copilot app, or Copilot CLI, powered by GPT Image 2.5 Flare; results preview inline and save directly to your workspace. Organization and enterprise owners can disable image generation via Copilot model policies (Organization Settings > Copilot > Policies > Model policies), and users can opt in to a visible `Made with AI` watermark on generated/edited images, off by default.

▶ Watch video

Disable image generation for your organization to prevent AI-generated images from being produced by Copilot users.

📍 In GitHub: go to Organization Settings › Copilot › Policies › Model policies, then disable the image generation model.

— Names model, policy path, and watermark default.

Generate and edit images directly in Co… | GitHub Copilot app, Universe releases (…

09 Cross-repository code search via /research NEW 81

Use `/research` in Copilot to search for exact text, symbols, regex patterns, or natural-language descriptions across multiple repositories without a local clone, narrowing results by repository, path, or language.

Trace retry behavior scattered across a payments service, shared library, and background workers before making changes.

```
$ /research How do these components retry failed charges, and where could retries overlap?
```

Plan a cross-repository API migration by finding all callers and implementations of the old API before writing any code.

```
$ /research Identify all repositories still calling the old payment API and list the changes each service needs to migrate.
```

— Exact command with concrete search scopes; no limits specified.

GitHub intelligence puts your code, con…

10 Customizations Marketplace for agent skills and plugins NEW 78

Discover, create, and manage agent customizations — skills, MCP servers, plugins — from the Customizations Marketplace in the Agents window sidebar or via the `Chat: Open Customizations` command (enabled by default in preview). Register plugin marketplaces and enable default plugins at the repository level via `.github/copilot/settings.json`.

— Exact command and config file path named. GitHub Copilot in VS Code, Universe rel…

11 **Copilot access bundled into GitHub Enterprise** IMPROVED 70

GitHub Enterprise now includes Copilot access for every licensed user, replacing separate seat and usage tracking with a single enterprise budget metered from the first request; code completion and next edit suggestions keep working after the budget is exhausted, while Copilot Chat, Copilot code review, and Copilot in the cloud require available budget. Users in an enterprise account without a GitHub Enterprise license can get the same features and models via Copilot Standalone at $10 per user per month, with no monthly AI credits per seat.

— Concrete pricing and budget mechanics, but no setup command.

GitHub Enterprise now includes access t…

12 **Copilot Memory generally available** IMPROVED 60

GitHub Copilot Memory is now generally available on paid Copilot plans, letting Copilot remember personal preferences and repository conventions across sessions in the Copilot app, Copilot CLI, VS Code, Copilot cloud agent, Copilot code review, Slack, Teams, and GitHub Mobile.

— Names all supported surfaces but gives no setup steps.

GitHub intelligence puts your code, con…

THINNER COVERAGE BELOW

13 **Copilot connectors for external context** NEW 55

Bring context from services such as Slack, Notion, and Microsoft Learn into agent sessions without an MCP server using Copilot connectors, available in preview from the Browse page on all Copilot plans.

— Names services and entry point, no setup steps given.

GitHub Copilot in VS Code, Universe rel…

14 **Projects multi-repo workspace in Copilot app** NEW 45

The Copilot app now supports Projects (public preview), a workspace spanning multiple repositories and sessions that coordinates multiple agents in parallel and returns results such as pull requests for review. Projects also support automations for repeatable tasks, such as triggering a workflow whenever a specific event occurs.

— Describes the workflow but gives no navigation or config detail.

GitHub Copilot app, Universe releases (…

15 **Model comparison in the Agents window** NEW 45

Run models and harnesses in parallel in the Agents window, review results side by side, ask a Judge model to recommend a solution, or choose Synthesize to combine ideas. Model comparison is in preview.

·

— Describes behaviour but no exact command or setting given.

GitHub Copilot in VS Code, Universe rel…

16 **Copilot CLI installation via VS Code** NEW 40

Install GitHub Copilot CLI through the VS Code installer on Windows, when adding VS Code to your path on macOS, or by running `copilot` on Linux.

·

— Install paths named but thin on mechanism. GitHub Copilot in VS Code, Universe rel…

WAS THIS USEFUL? 👍 👎

GitLab

Feedback ⓘ

What happens when vulnerabilities are discovered faster than you can fix them? (2026-10-

BLOG ↗

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

GitLab adds Orbit context graph, Secrets Manager per-job credential scoping, and agentic remediation via Duo Agent Platform with sandboxed agent identities.

GitLab adds Orbit, a live context graph of the software lifecycle that connects findings to the changes that introduced them, the pipelines that shipped them, and the teams who own the fix, enabling exposure questions like reachability and blast radius to be answered across thousands of repositories.

GitLab adds Secrets Manager, which limits each pipeline job to only the credentials it explicitly requests and is authorized to use, so a compromised dependency can reach only the secrets of the job it runs in.

GitLab Duo Agent Platform now gives each agent a composite identity limited to the permissions it shares with the requesting user, a sandbox destroyed when the task ends, and a full action record, with agents earning more autonomy only as controls at each stage are proven under the GitLab Security Standard.

GitLab Duo Agent Platform now investigates findings in application context, filters likely false positives, prioritizes by exploitability and reachability, writes a fix, runs it through the pipeline for regression and security scan checks, and surfaces the change, explanation, and pipeline results in a single merge request for developer review.

GitLab's Dependency Firewall now blocks policy-violating packages before they enter the build, preventing vulnerable or malicious open-source dependencies from reaching production.

NEW DETECTION Business Logic Security Analyzer

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ SAST updates (2026-10-28) BLOG ↗

Veracode is a cloud-based application security platform that scans code, binaries, and running applications to find and help remediate software vulnerabilities.

Veracode SAST adds C# and Java source code scanning, a DryRun Security integration, Pipeline Scan support for artifacts over 200 MB, and `veracode.json` `-based` exclusions for Java `.jar` files and classes.

NEW SUPPORTED PLATFORM Scan C# source code directly (Static Analysis Engine v2026.10).

NEW SUPPORTED PLATFORM NEW DETECTION Scan Java source code and view it on the platform, using `veracode.json` to exclude specific `.jar` files or classes from analysis.

NEW SUPPORTED PLATFORM Pipeline Scan now accepts packaged artifacts larger than 200 MB with no changes to existing integrations.

NEW INTEGRATION Veracode SAST now integrates with DryRun Security, surfacing findings and remediation guidance during pull request and code review workflows.

NEW SUPPORTED PLATFORM Scala 3.9 support

UPDATED SUPPORTED PLATFORM Android 16 support enhanced

NEW SUPPORTED PLATFORM iOS 27 support

NEW SUPPORTED PLATFORM Go 1.27 support

NEW SUPPORTED PLATFORM Dart 3.13 and Flutter 3.47 support

NEW SUPPORTED PLATFORM PHP 8.4 and PHP 8.5 support

NEW SUPPORTED PLATFORM Next.js 16.x support

NEW SUPPORTED PLATFORM Python google-cloud-bigquery library support

NEW SUPPORTED PLATFORM Enhanced Python scanner with PySpark, Flask, Django, FastAPI support

NEW SUPPORTED PLATFORM Android 17 support

NEW SUPPORTED PLATFORM React 19 support

NEW SUPPORTED PLATFORM Kotlin 2.3 support

NEW SUPPORTED PLATFORM Psycopg 3 support in Python

NEW SUPPORTED PLATFORM Xcode 26.4 support

NEW SUPPORTED PLATFORM Dart 3.11 and Flutter 3.41 support

NEW SUPPORTED PLATFORM JDK 26 support

NEW SUPPORTED PLATFORM Angular 20 and Next.js 15.x support

NEW SUPPORTED PLATFORM Go Fast HTTP support

NEW SUPPORTED PLATFORM CloudKit framework support on Apple platforms

NEW SUPPORTED PLATFORM Apple Security framework APIs support

NEW SUPPORTED PLATFORM Go 1.26 support

NEW SUPPORTED PLATFORM PyYAML support in Python

NEW SUPPORTED PLATFORM Apex 64 and Apex 65 support

NEW SUPPORTED PLATFORM Spring Boot 4, Spring Core 7, Spring Security 7 support

NEW SUPPORTED PLATFORM Ruby 4.0 and Rails 8.1 support

NEW SUPPORTED PLATFORM Svelte framework support in JavaScript

NEW SUPPORTED PLATFORM .NET 10 support

NEW SUPPORTED PLATFORM Dart 3.10 and Flutter 3.38 support

NEW SUPPORTED PLATFORM Go Fiber web framework support

NEW SUPPORTED PLATFORM Kotlin 2.4 support

NEW SUPPORTED PLATFORM Dart 3.12 and Flutter 3.44 support

NEW DETECTION Hardcoded values in Dart getter functions

NEW DETECTION CWE-295 and CWE-297 detection via httplib in Python

NEW DETECTION CWE-73 taint sinks for send_from_directory and send_file in Python

NEW DETECTION CWE-80 taint sink coverage for .NET System.Web.UI.Page.Title and HtmlHead.Title

UPDATED DETECTION Enhanced Python scanner taint tracking and cross-file analysis

---

WAS THIS USEFUL? 👍 👎

Waratek

Feedback ⓘ

Waratek Unveils AI Phylax at Oracle AI World: A Runtime Guardian That Stops Attacks on Ja

BLOG ↗ RANK

Waratek is a compiler-based IAST and RASP that report 100% of exploitable vulnerabilities before production and block attacks-including zero-days-at runtime, no code changes.

> Waratek introduced AI Phylax, a runtime guardian that enforces deterministic security rules to stop prompt injection and tool hijacking attacks on Java-based AI agents.

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

01 AI Phylax runtime guardian for Java AI agents NEW

37

AI Phylax is a new runtime guardian that enforces immutable security rules to block prompt injection and tool hijacking attacks against Java-based AI agents. It applies deterministic protection—the same security rule produces the same outcome every time—giving security teams certainty against attacks regardless of phrasing or origin, without disrupting legitimate agent behavior.

– Explains behavior and intent but no config, API, or deployment detail.

Waratek Unveils AI Phylax at Oracle AI …

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

GitGuardian SaaS

Feedback ⓘ changelog · Oct 29, 2026

CHANGELOG ↗ RANK

GitGuardian SaaS is a cloud-hosted security platform that detects exposed secrets, API keys, and credentials in source code repositories and developer workflows.

> GitGuardian SaaS adds a local machine dashboard Overview page and a low-priority `--background` scan mode for ggshield, extends monitoring to Docker Hub with GitHub-parity incident handling, enriches Wiz findings with GitGuardian IDs, brings honeytokens to Windows, skips more build-cache folders during scans, and restricts validity-check custom hosts to workspace-only configuration.

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

01 **Low-priority background scan mode** NEW 90

A new `--background` flag (e.g. `ggshield machine report --background`) runs machine scans at low priority so they don't slow developer machines; it can also be made the default fleet-wide via `scan.resources.background.mode: auto` set in a config file such as `machine_scan.yaml`.

Add to a scheduled MDM scan command so the scan runs at low priority without slowing developer machines.

```
$ ggshield machine report --background
```

Make low-priority background mode the default for all machine scans fleet-wide, so no per-command flag is needed.

```yaml
scan:
  resources:
    background:
      mode: auto
```

— Flag, config key, and config file named with runnable commands.

changelog-20261029-a7633d5e

02 **Docker Hub incident monitoring** NEW 65

Docker Hub incidents now carry publishing account, image, repository, and layer context, and flow through the same notifications, integrations, and agents analysis as GitHub incidents.

— Describes new source and parity with GitHub, but only a UI screenshot as starting point.

changelog-20261029-a7633d5e

03 **GitGuardian IDs in Wiz findings** IMPROVED 60

Findings pushed to Wiz now include GitGuardian incident, occurrence, and source IDs in the finding's `originalObject` field, for use in Wiz workflows and the Wiz API.

— Names the exact field but no example of using it. changelog-20261029-a7633d5e

THINNER COVERAGE BELOW

04 **Scans skip more build-cache folders** IMPROVED 55

Scans now skip additional folders of downloaded or generated files, including `pip-*`, `pytest-of-*`, and `_MEI*` temp leftovers, NuGet and Scoop package caches, and Electron app caches.

— Names exact skipped patterns but change is automatic, no action needed.

changelog-20261029-a7633d5e

05 **Honeytoken planting on Windows** NEW 25

Honeytoken planting is now supported on Windows endpoints.

— Single-sentence mention with no mechanism or usage detail. changelog-20261029-a7633d5e

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! Validity checks no longer read custom hosts from environment variables or local config files; custom hosts are now sourced exclusively from your GitGuardian workspace.

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

Socket

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗ RANK

Socket is a supply chain security platform that analyzes open-source package dependencies (npm, PyPI, etc.) to detect malicious code, risky behaviors, and vulnerabilities before developers install them.

> Socket is retiring a legacy report-view API endpoint and changing how the Obfuscated code alert is applied by default in security policy presets, both effective in November 2026.

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

01 Report view endpoint migration to full-scans API

DEPRECATED

88

The `GET /v0/report/view/{id}` endpoint is deprecated and will be retired on November 20, 2026; it now returns a Sunset response header advertising the retirement date. Integrations must migrate to `GET /v0/orgs/{org_slug}/full-scans/{full_scan_id}` to continue retrieving scan reports.

Check the new full-scans endpoint to retrieve a scan report after the old view endpoint is retired.

```
$ curl -s -H 'Authorization: Bearer <token>'
'https://api.socket.dev/v0/orgs/<org_slug>/full-
scans/<full_scan_id>'
```

Verify the Sunset header on the deprecated endpoint before your migration deadline to confirm the retirement date.

```
$ curl -sI -H 'Authorization: Bearer <token>'
'https://api.socket.dev/v0/report/view/<id>' | grep -i sunset
```

— Exact deprecated and replacement endpoints with migration deadline and header check

changelog-20261029-548bc6c8

02 Obfuscated code alert removed from default policy presets

72

BREAKING

Starting November 10, 2026, the Obfuscated code alert will be removed from the Balanced and Comprehensive security policy preset defaults. Organizations that want

to keep receiving it must open Security Policy and set `Obfuscated code` to `Warn` or `Monitor` instead of `Inherit`, or add a matching rule on the Policies page.

— Names exact UI settings and deadline but no API/config key `changelog-20261029-548bc6c8`

└──▷ BREAKING ON UPGRADE

! The `GET /v0/report/view/{id}` endpoint is retired on November 20, 2026; integrations using it must switch to `GET /v0/orgs/{org_slug}/full-scans/{full_scan_id}`.

! The `Obfuscated code` alert is removed from the `Balanced` and `Comprehensive` security policy presets on November 10, 2026; organizations relying on preset defaults will stop receiving this alert unless they explicitly set it to `Warn` or `Monitor`.

WAS THIS USEFUL? 👍 👎

OX Security

Feedback ⓘ

Introducing Agent Activity: See What Your AI Agents Are Actually Doing (2026-10-28)

BLOG ↗ RANK

Ox security is a accelerate the transition to software that secures itself. OX Security pinpoints risk to the exact line of code, eliminating security debt from AI generation to cloud runtime.

> OX Security launches Agent Activity, an early-access runtime tracing and guardrail system for AI agents spanning `OX.VibeSec` and OX.Cloud, plus a new LiteLLM connector to pull proxy traffic into that visibility.

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

01 **Custom runtime guardrails for AI agents** NEW 72

Build custom runtime guardrails scoped to specific AI models, MCP servers, and skills, choosing to flag or block violations at a severity level you set. Agent governance can start from 100+ built-in out-of-the-box security policies covering runtime agent behavior, configured under Agent Activity > Guardrails.

Block a specific model from combining an MCP server with a skill that reaches sensitive internal data, before it can reach production.

> 📍 In `OX.VibeSec` or OX.Cloud, go to Agent Activity › Guardrails, create a custom policy scoped to the target model and MCP server, add the sensitive-data skill condition, and set the enforcement action to `block` with the severity level that fits your risk tolerance.

— Named scopes and actions with a concrete UI navigation path

Introducing Agent Activity: See What Yo…

02 **Agent Activity session tracing** NEW 67

OX Security now traces each AI agent session step by step via the new Agent Activity feature, covering prompts and responses, MCP server and tool calls, read/write access permissions, and sensitive data touches (PII, secrets, tokens, financial data). It is in early access on `OX.VibeSec` and OX.Cloud.

Investigate what an AI agent did during a suspicious session — trace its prompts, MCP calls, and sensitive data touches in one view.

> 📍 In `OX.VibeSec` or OX.Cloud, go to Agent Activity, select the agent session of interest, and review the full chain of prompts and responses, MCP server and tool calls, and any sensitive data (PII, secrets, tokens, financial data) touched during the session.

— Clear mechanism and scope, but UI-only path, no API/flag named

Introducing Agent Activity: See What Yo…

THINNER COVERAGE BELOW

03 **LiteLLM connector for agent visibility** NEW 33

Adds a LiteLLM connector to bring LLM proxy traffic into OX Security's agent visibility picture.

— Names the connector but no setup steps or detail on data captured

Introducing Agent Activity: See What Yo…

WAS THIS USEFUL? 👍 👎

cyclonedx-python

Feedback ⓘ v7.6.0 NOTES ↗ RANK

CycloneDX Software Bill of Materials (SBOM) generator for Python projects and environments

> cyclonedx-python added a flag to isolate SBOM generation from the host shell's Python environment variables.

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

01 **Environment isolation flag for environment command** NEW 75

The `environment` command now supports a `-E` flag that ignores all inherited `PYTHON*` environment variables during SBOM generation, useful for isolating generation from the host shell (e.g. in CI where those vars may point to the wrong interpreter). Example: `cyclonedx-py environment -E .venv`.

Generate an SBOM from a virtual environment without inheriting the host shell's `PYTHON*` variables, useful in CI where those vars may point to the wrong interpreter.

```
$ cyclonedx-py environment -E .venv
```

— Names exact flag and command with runnable example v7.6.0

WAS THIS USEFUL? 👍 👎

StepSecurity

Feedback ⓘ Dev Machine Guard v1.18.1 (2026-10-28)

BLOG ↗

StepSecurity is a security platform that hardens CI/CD pipelines, such as GitHub Actions, by detecting supply-chain risks, enforcing least-privilege runners, and monitoring workflow tampering.

Adds automatic MSI self-updates with rollback, configurable device identity via `device_id` in `config.json`, and a `--disable-runtime-scan` flag.

Opt out of automatic MSI self-updates at install time with `AUTOUPDATE=0`; when enabled, the agent verifies SHA-256 hash, signed checksum, and Authenticode publisher before updating, rolls back automatically on failure, and never retries a bad version.

NEW SUPPORTED PLATFORM Turn off language runtime scanning by setting `enable_runtime_scan` to `false` in the agent configuration or passing `--disable-runtime-scan`; scanning is on by default.

Set a custom `device_id` in the agent's `config.json` to give a device a stable, admin-controlled identity used by scans, scheduling, hooks, and device policies.

NEW SUPPORTED PLATFORM Windows system package inventory

NEW INTEGRATION Package inventory for Go, Rust, PHP, .NET, and Ruby ecosystems

NEW INTEGRATION GitHub Copilot plugin inventory in Agent Plugins

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

PortSwigger Burp Suite

Feedback ⓘ

DAST 2026.10.3 (2026-10-29) 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 DAST added API scanning from captured Burp XML and HAR files and clarified GraphQL scan configuration.

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

01 **API site creation from Burp XML and HAR files** NEW

55

Burp Suite DAST can now create an API site directly from Burp XML and HAR files, allowing APIs captured in those formats to be scanned.

— Names formats but no steps or limits given DAST 2026.10.3 (2026-10-29)

02 **Clearer GraphQL API URL guidance** IMPROVED

20

Burp Suite DAST now makes it clearer which URL to enter when configuring a GraphQL API scan.

— Vague UI clarification with no specifics DAST 2026.10.3 (2026-10-29)

WAS THIS USEFUL? 👍 👎

◆ WAF, Bot & API Protection

DataDome

Feedback ⓘ Node.js module 2.7.0 (2026-10-28) BLOG ↗

RANK

DataDome protects web, mobile, and API applications by detecting and blocking bot and fraud traffic.

> DataDome's Node.js module 2.7.0 adds TLS fingerprint collection to strengthen bot-detection signals, alongside a small TypeScript typing update.

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

01 **TLS fingerprint collection for bot detection** NEW 35

DataDome now collects TLS fingerprints from incoming requests and sends them as richer bot-detection signals to the Bot Protect API.

— Explains what's collected and where it's sent, but no config or flag given

Node.js module 2.7.0 (2026-10-28)

02 **RequestMetadata TypeScript type added** NEW 35

DataDome now includes the `RequestMetadata` property in the TypeScript type definitions.

— Names exact type property but no usage detail Node.js module 2.7.0 (2026-10-28)

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

Unfurl

Feedback ⓘ v2026.11 NOTES ↗ CODE ↗ RANK

Extract and Visualize Data from URLs using Unfurl

> Unfurl adds forensic parsers for ETags, ChatGPT/OpenAI IDs, and Firebase Push IDs, and switches timestamp conversion to integer math for better precision.

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

01 ETag parser for file metadata NEW

88

Unfurl now parses ETags found in `etag` query parameters or quoted header values (`"..."` or `W/"..."`), decoding layouts from Apache httpd, nginx, and Node.js to extract file size, mtime (in seconds, milliseconds, or microseconds), inode, and compression suffix.

Decode an image URL containing an Apache-style ETag in a query parameter to recover the origin file size and modification time.

```
$ unfurl "https://example.com/image.jpg?etag=%22f4381-6385a594%22"
```

— Names exact source formats and fields, plus a runnable example v2026.11

02 Integer-based timestamp conversion precision IMPROVED

69

Unfurl now converts WebKit, WebKit milliseconds, Windows FileTime, and UUID v1/v6 timestamps using integer math instead of floating-point, preserving source precision (three digits for WebKit milliseconds, six for WebKit, seven for FileTime and UUID times).

— Explains mechanism and precision numbers but no usage example v2026.11

THINNER COVERAGE BELOW

03 New ID parsers for ChatGPT/OpenAI and Firebase NEW

32

Unfurl now parses `ChatGPT` and `OpenAI` IDs embedded in URLs, and separately parses Firebase Push IDs embedded in URLs.

— Names the ID types but no mechanism or example given v2026.11

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Chainguard

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗

Chainguard provides trusted open source artifacts for every layer of your modern software stack—containers, language libraries, and VM images.

- NEW SUPPORTED PLATFORM Rancher 2.11 hardened images
- NEW SUPPORTED PLATFORM GitLab EE commercial images with FIPS variants
- NEW SUPPORTED PLATFORM Sentry suite hardened images
- NEW SUPPORTED PLATFORM apache-pulsar:4.0 hardened image
- NEW SUPPORTED PLATFORM Additional new hardened images

WAS THIS USEFUL? 👍 👎

kubescape

Feedback ⓘ v4.0.17 NOTES ↗ RANK

Kubescape is an open-source Kubernetes security platform for your IDE, CI/CD pipelines, and clusters. It includes risk analysis, security, compliance, and misconfiguration scanning, saving Kubernetes users and administrators precious time, effort, and resources.

> Kubescape v4.0.17 expands its MCP server with new vulnerability, posture, SBOM, and remediation tools, adds fleet configuration files with graded exit codes, and enriches image scan output with CISA KEV/EPSS scores, webhook notifications, and Gateway API-aware exposure analysis.

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

01 Expanded MCP server tools for vulnerability and posture queries

IMPROVED 90

The MCP server gains new tools: `create_admission_policy_binding`, `list_configuration_security_scan_summaries`, `list_sboms`, `list_sbom_packages`, and `validate_scan_selection` (with shared control resolution). Existing tools are extended — `analyze_vulnerability_exposure` gains an `include_identity` parameter, `list_vulnerabilities_in_manifest` gains filtering and pagination, `get_configuration_security_scan_manifest` gains control filtering, `list_controls` can be filtered by framework and paginated, and `diff_reports` counts unchanged findings while listing them only on request. Remediation for report items from posture reports can now be applied via MCP.

— Names every tool and parameter but no runnable client example v4.0.17

02 Webhook notifications for image scans NEW

85

The image scan command gains a `--notify` flag that posts a webhook to a given URL after the scan completes, letting downstream systems receive vulnerability results automatically.

Trigger a webhook after scanning an image so a downstream system receives the vulnerability results automatically.

```
$ kubescape scan image nginx:latest --notify
https://hooks.example.com/kubescape
```

— Exact flag plus a runnable command example v4.0.17

03 Helm rendering improvements in fix command IMPROVED

80

The `fix` command adds an `--output-post-renderer` flag for Helm, hardens overlay staging and boundaries, and renders Helm charts targeting the newest Kubernetes version allowed by the chart's `kubeVersion`.

— Named flag and concrete behaviour change, no sample invocation v4.0.17

04 **Gateway API ReferenceGrant support in exposure analysis** NEW

60

Exposure analysis now evaluates Gateway API `ReferenceGrant` objects to correctly account for cross-namespace backends when determining exposure.

— Names the object evaluated but no command to try it v4.0.17

THINNER COVERAGE BELOW

05 **Fleet config file and graded exit codes** NEW

50

Fleet runs can now read their settings from a config file (`feat(fleet): read fleet settings from a config file`), and fleet runs emit graded exit codes reflecting scan outcomes.

— Config file and exit codes named but no exact key or code values v4.0.17

06 **CISA KEV and EPSS scores in image scan output** NEW

50

Image scan output now includes CISA Known Exploited Vulnerabilities (KEV) flags and EPSS exploit prediction scores for each vulnerability, helping prioritize remediation.

— Describes the data added but no field name or flag v4.0.17

07 **Exception audit trail in SARIF results** IMPROVED

32

SARIF scan results now retain an audit trail of exceptions applied, preserving the history of suppressed or excepted findings.

— One-line description with no mechanism or location detail v4.0.17

└──▷ ALSO FROM THESE RELEASES

Pipe a local manifest into the predict subcommand from stdin instead of passing a file path — useful in CI pipelines where the manifest is generated on the fly.

```
$ helm template my-release ./chart | kubescape predict -
```

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

Sysdig Secure

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗

RANK

Sysdig Secure is a cloud security platform that provides runtime threat detection, vulnerability management, and compliance monitoring for containers, Kubernetes, and cloud workloads.

> Sysdig Secure extends vulnerability scanning to standalone binaries (including source-compiled PHP) across its Registry and Agentless Host scanners, broadens risk acceptance to cover non-package components, and previews license detection for scanned packages.

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

01 Standalone binary scanning for PHP across scanners

BREAKING

62

Registry Scanner v0.13.0 adds standalone binary scanning to identify applications not installed by a package manager, including PHP compiled from source, letting distroless and scratch images surface new findings after upgrade. Agentless Host Scanning now also identifies PHP in standalone binaries, including PHP compiled from source such as the official Docker Hub `php` images, with no new deployment steps required. Because this can surface findings on images that previously showed none, Sysdig recommends reviewing results after upgrading Registry Scanner.

⋮

– Names versions and images affected, but no CLI/API detail changelog-20261029-21dc9b7d

THINNER COVERAGE BELOW

02 Risk acceptance for non-package components in CLI Scanner

IMPROVED

41

CLI Scanner v1.31.0 extends risk acceptance to every component type, so accepted risks now apply to vulnerabilities found in standalone binaries and other components that are not packages.

– States scope change but no mechanism or UI path changelog-20261029-21dc9b7d

03 License detection for scanned packages NEW

37

Registry Scanner v0.13.0 adds license detection for packages in scanned images, available in Technical Preview under License Classification.

– Names feature and preview status but little else changelog-20261029-21dc9b7d

└──▷ **BREAKING ON UPGRADE**

! Registry Scanner v0.13.0 standalone binary scanning may surface new findings on images (distroless, scratch) that previously showed none — review results after upgrading.

WAS THIS USEFUL? 👍 👎

◆ **CNAPP**

Plerion

Feedback ⓘ Exempt findings from your infrastructure as code:

NOTES ↗

Plerion is a cloud security platform that detects misconfigurations, vulnerabilities, and threats across cloud environments and provides remediation guidance.

Plerion now supports exemptions for IaC findings, scoped to a full repository or a single file, persisting across future scans.

Exempt IaC findings by choosing Exempt on a finding or adding a name exemption to the code integration's profile, scoped to a repository (e.g. `my-org/infra`) or a single file (e.g. `my-org/infra/s3.tf`), persisting on every later scan.

UPDATED VULNERABILITY CHECK Code Security checks now support exemptions

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SIEM

Cisco Splunk Enterprise

Feedback ⓘ

changelog · Oct 29, 2026 NOTES ↗ RANK

Splunk Enterprise enables you to search, analyze and visualize your data to quickly act on insights from across your technology landscape.

> Splunk Enterprise 8.2 introduces Federated Search across deployments, a new Dashboard Studio experience, durable scheduled reports, expanded JSON data handling in search, and replaces SSL compression with HTTP compression by default.

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

01 JSON data handling in search with tojson and eval functions

NEW 90

Adds the `tojson` search command plus four new JSON eval functions — `json_array_to_mv`, `mv_to_json_array`, `json_append`, and `json_extend` — to convert, append to, and extend JSON-structured data within a search pipeline.

Convert raw log events into JSON-structured data inline during a search for downstream processing or indexing.

```
$ index=main sourcetype=syslog | tojson
```

Append a new element to an existing JSON array field and extend a JSON object with array values in a single search pipeline.

```
$ index=main | eval tags=json_append(tags, "new_tag") | eval
metadata=json_extend(metadata, tag_array)
```

– Named commands/functions with runnable example commands 2026-10-29-b4054ba7

02 HTTP compression replaces SSL compression by default

BREAKING 60

Splunk Enterprise now uses HTTP compression by default in place of SSL compression, reducing the security vulnerability surface; this does not apply to forwarding, and deployments relying on SSL compression need to review their configuration.

– Clear before/after but no exact config key given 2026-10-29-b4054ba7

03 **Health report monitoring enhancements** IMPROVED 60

Health report gains new capabilities: monitoring ingestion latency to detect when forwarders have fallen behind, identifying excessive disk I/O wait times via the new IOWait feature with status written to `health.log`, and capturing feature health status across nodes in distributed environments including search head cluster members.

— Names health.log and IOWait but lacks commands to view status 2026-10-29-b4054ba7

THINNER COVERAGE BELOW

04 **Workload Management rule control and OOM messaging** IMPROVED 50

Workload Management now lets you enable or disable individual workload rules and admission rules, and displays a default message when it terminates a search due to an out-of-memory (OOM) condition.

— Describes new controls but no exact command or UI path 2026-10-29-b4054ba7

05 **Durable Search for scheduled reports** NEW 45

The new Durable Search feature ensures at-least-once delivery of events for scheduled reports, automatically rerunning incomplete reports.

— Explains mechanism but no configuration steps given 2026-10-29-b4054ba7

06 **Federated Search across deployments** NEW 40

Run Federated Search across multiple Splunk Enterprise and Splunk Cloud Platform deployments from a single interface.

— Describes capability but no setup detail or syntax 2026-10-29-b4054ba7

07 **Dashboard Studio dashboard experience** NEW 35

Build and customize dashboards with Dashboard Studio, a new dashboard experience offering advanced visualization tools and fully customizable layouts.

— Named feature but no UI path or configuration specifics 2026-10-29-b4054ba7

└──▷ **BREAKING ON UPGRADE**

! SSL compression is replaced with HTTP compression by default except when forwarding — deployments relying on SSL compression will need to review their configuration.

WAS THIS USEFUL? 👍 👎

Databricks

Feedback ⓘ

Serverless GPU for clean room notebooks is now generally available (2026-10-28)

BLOG ↗ RANK

Databricks is a cloud-based data lakehouse platform for data engineering, analytics, machine learning, and AI workloads, built on Apache Spark.

> Databricks shipped GA serverless GPU compute for clean room notebooks (with an opt-in toggle ahead of its default rollout) and launched the Unity Gateway Usage Dashboard v1.0 for tracking coding-agent spend and adoption.

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

01 Serverless GPU compute for clean room notebooks NEW

72

Clean room notebooks can now run on serverless GPU compute for model inference and training over shared data, using AI Runtime with the same approval flow, data access, and output tables as other clean room notebooks. This is generally available now, and will become the default for accounts where it's off starting November 26, 2026; teams can opt in early by enabling Clean Rooms AI Runtime from the Previews page in the account console.

.
.
.
.

Turn on serverless GPU for clean rooms early, before the automatic November 2026 rollout, so your team can run notebooks on GPU compute within a clean room now.

> 📍 In the account console, go to Previews and enable Clean Rooms AI Runtime.

— Names the toggle and rollout date but mechanism is brief

Serverless GPU in clean rooms will soon… Serverless GPU for clean room notebooks…

02 Unity Gateway Usage Dashboard v1.0 NEW

60

A new Usage Dashboard for Unity Gateway tracks coding-agent adoption, harness usage, and estimated session spend, and supports tag-based spend attribution plus expanded model and user spend analysis. Accessible via Unity Gateway > Usage Dashboard in the Databricks console.

Navigate to the Unity Gateway Usage Dashboard to review coding-agent adoption and session spend broken down by tag, model, and user.

> 📍 In the Databricks console, go to Unity Gateway › Usage Dashboard to explore coding-agent adoption, harness usage, estimated session spend, and tag-based

spend attribution.

— Names dashboard features and navigation but no API or config detail

Unity Gateway Usage Dashboard v1.0 (202…

WAS THIS USEFUL? 👍 👎

Sumo Logic Feedback ⓘ

JSON Unroll for HTTP Log Sources (Collection) (2026-10-28) BLOG ↗ RANK

Sumo Logic is a cloud-native machine data analytics platform that collects, searches, and analyzes logs and metrics for security monitoring, troubleshooting, and operational insights.

> Sumo Logic's HTTP log sources now automatically unroll JSON arrays into individual log messages.

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

01 **JSON Unroll for HTTP log sources** NEW 45

HTTP log sources automatically split JSON arrays into individual log messages while preserving top-level metadata.

— Explains behaviour but no config key or flag given

JSON Unroll for HTTP Log Sources (Colle…

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

SigmaHQ sigma-cli

Feedback ⓘ v4.0.0 NOTES ↗ RANK

The Sigma command line interface based on pySigma

> sigma-cli v4.0.0 introduces a security policy system for rule conversion and validation, defaulting to a safer RE2-based mode, and migrates its underlying library to pySigma 2.

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

01 Security policy system for convert and check

BREAKING

93

New `--policy safe` (default) and `--policy trusted` options on both the `convert` and `check` commands control how risky rule content is processed: safe mode uses the RE2 regex engine, disables template variable expansion, and blocks external rule sources. The regex engine can be overridden independently of policy with `--regex-engine re2` or `--regex-engine python`; template variable expansion can be re-enabled with `--enable-template-vars` (emits a security warning); and external rule sources can be explicitly permitted with `--allow-external-sources`. Because `safe` is now the default, existing scripts relying on Python-native regex, template variables, or external sources will break unless `--policy trusted` or the relevant individual flags are added.

Convert untrusted community rules with the safe default policy to guard against regex DoS — no extra flags needed; RE2 and blocked external sources are on by default.

```
$ sigma convert -t splunk -p sysmon --policy safe
sigma/rules/windows/process_creation
```

Convert rules from a trusted internal library that use template variables and Python-native regex patterns — upgrade from v3 behaviour by passing `--policy trusted --enable-template-vars`.

```
$ sigma convert -t splunk -p sysmon --policy trusted --enable-
template-vars sigma/rules/windows/
```

Validate a rule set with `check` while keeping the safe policy but explicitly allowing external sources for a controlled pipeline environment.

```
$ sigma check --policy safe --allow-external-sources
sigma/rules/windows/process_creation/
```

— Names every flag, default behaviour, and migration path with runnable examples. v4.0.0

THINNER COVERAGE BELOW

02 **Migration to pySigma 2** IMPROVED 25

sigma-cli now uses pySigma 2 as its underlying library.

— No detail on what changed beyond the version bump. v4.0.0

└──▷ **BREAKING ON UPGRADE**

! The default policy is now `safe`, which switches the regex engine to RE2, disables template variable expansion, and blocks external rule sources — existing scripts that rely on Python-native regex, template variables, or external sources will break unless `--policy trusted` (or the relevant individual flags) is added.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗ RANK

An asset discovery and inventory platform that identifies and maps all devices on networks without requiring agents.

> runZero's latest release adds LonTalk protocol discovery and configurable AI tool-call limits for self-hosted deployments, alongside broad search improvements across inventories, alerts, scan templates, and the account API.

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

01 AI tool-call limits per turn NEW

90

Self-hosted deployments can cap how many tool calls the LLM makes in a single turn using the `RUNZERO_LLM_MAX_TOOL_CALLS_PER_TURN` and `RUNZERO_LLM_MAX_TOOL_CALLS_PER_DEEP_TURN` environment variables (defaults: 8 and 20), and per-account or per-organization limits can also be set through the AI configuration pages or the API.

Cap how many AI tool calls the LLM can make in a single turn on a self-hosted console to prevent runaway agentic queries.

```
$ RUNZERO_LLM_MAX_TOOL_CALLS_PER_TURN=4
RUNZERO_LLM_MAX_TOOL_CALLS_PER_DEEP_TURN=10 ./runzero-console
```

— Exact env vars, defaults, and runnable command given changelog-20261029-8eca0c43

02 API 422 errors for unparseable searches IMPROVED

90

The `GET /api/v1.0/account/sites`, `GET /api/v1.0/account/orgs`, and `GET /api/v1.0/account/credentials` APIs now return a 422 error naming the problem when a search cannot be parsed, rather than returning every record.

— Exact endpoints, methods, and status code named changelog-20261029-8eca0c43

03 Search operator improvements across inventories IMPROVED

80

The `search` operator across the asset, service, software, and vulnerability inventories is now case-insensitive; exact-match searches like `domain:=corp.example.com` now find assets that have that domain among others; and `product:=` and `domain:=` now match assets with no products or no domains.

— Exact query syntax and before/after behaviour given changelog-20261029-8eca0c43

04 **Alert channel search fields** NEW 80

Alert channel searches using `settings:`, `notification_count:`, and `user_email:` now work; `settings:` matches a channel's email recipients and `notification_count:` accepts numeric comparisons such as `notification_count:>5`.

Filter alert channels with more than five notifications to identify noisy rules during tuning.

```
$ notification_count:>5
```

— Named search fields with a runnable query example changelog-20261029-8eca0c43

05 **Boolean search in scan templates and reports** IMPROVED 60

Search in scan templates and external reports now supports `AND`, `OR`, and `NOT` operators; in scan templates a plain word searches template names and descriptions, and an unsupported keyword is reported as an error.

— Operators named but no example query shown changelog-20261029-8eca0c43

THINNER COVERAGE BELOW

06 **Tag editing in asset details card** NEW 45

Tag editing is now available directly in the asset details card on the Vulnerability details page.

— UI path given, no further mechanism described changelog-20261029-8eca0c43

07 **LonTalk protocol discovery support** NEW 30

runZero now supports the LonTalk protocol for asset discovery.

— Bare mention, no scan config or mechanism detail changelog-20261029-8eca0c43

WAS THIS USEFUL? 👍 👎

syzkaller

Feedback ⓘ changes since 2026-10-26 CODE ↗

syzkaller is an unsupervised coverage-guided kernel fuzzer

syzkaller adds `http_public_url` option to syz-manager and a `MaxRetries` field to `CollectRunsOpts` for infra-error back-off

└──▷ **USE IT**

Expose the syz-manager dashboard at a stable public address so external dashboards or CI systems can link directly to it.

```yaml
http_public_url: "https://fuzzer.example.com"
```

Configure a public-facing URL for the syz-manager HTTP interface with the new `http_public_url` option in `pkg/mgrconfig`.

Limit infra-error retries in `CollectRuns` with the new `MaxRetries` field on `CollectRunsOpts`; exceeding the limit now returns `ErrTooManyInfraErrors`.

syzkaller's aflow repro loop now tracks `LatestOracleFeedback` separately from the cumulative `OracleFeedback`, so the LLM generator receives only the most recent oracle result.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Management (UEM/RMM)

Fleet

Feedback ⓘ fleet-v4.94.0 NOTES ↗ RANK

Open device management

> Fleet v4.94.0 ships a config-profile management overhaul (new fields, dedicated edit page), self-service and hidden profiles, a customizable Windows EULA, per-device one-time Windows MDM enroll secrets, on-demand FileVault key rotation, and a broad sweep of GitOps, retention, and software/API improvements.

└──▷ **WHAT SHIPPED · 14 FEATURES** most completely described first ? what's the number?

01 Skip end-user auth at Windows MSI install time NEW

90

Adds a `BYPASS_END_USER_AUTH` property to the Windows MSI built by `fleetctl package`, letting admins skip end-user authentication at install time with `msiexec /i fleetd-base.msi BYPASS_END_USER_AUTH=true` instead of baking in `--bypass-end-user-auth`; requires fleetd v1.60.0 or higher.

— Runnable command with exact flag and version requirement fleet-v4.94.0

02 Configurable retention for MDM commands and host certificates

NEW

85

Adds configurable retention and cleanup to keep data from growing unbound: Windows MDM command-history retention via `mdm.windows_command_retention` (env `FLEET_MDM_WINDOWS_COMMAND_RETENTION`, default 30 days, `0` disables cleanup), deleted-host certificate retention via `server.deleted_host_certificates_retention` (default 30 days), and a new hourly cleanup job for completed Apple MDM commands.

Tune how long Fleet retains Windows MDM command history before purging it, or disable the cleanup entirely.

yaml

```yaml
mdm:
  windows_command_retention: 720h
```

— Named keys, env var, defaults, and config example fleet-v4.94.0

03 Customizable Windows end-user license agreement NEW

83

Admins can upload a Markdown EULA file up to 512 KB in Settings > Integrations > MDM > End user license agreement, or set `windows_eula` in GitOps YAML; Fleet renders it as the terms page during Microsoft Entra and Autopilot enrollment.

— Exact UI path, config key, and file size limit given `fleet-v4.94.0`

---

04 **Configuration profiles: name/description fields and dedicated edit page**

IMPROVED

80

Adds `name` and `description` fields to configuration profiles, settable via the UI, the API, or GitOps YAML, deprecating `display_name` on the batch configuration profiles endpoint in favor of `name`. Also adds a dedicated page for adding and editing configuration profiles — replacing the add and edit modals — with support for upload, paste, and inline editing.

— Names endpoint deprecation and UI change but no example `fleet-v4.94.0`

---

05 **Per-device one-time Windows MDM enroll secrets** NEW

80

New `mdm.windows_one_time_enroll_secrets` server setting sends each Windows MDM host a per-device, single-use enroll secret instead of the shared global secret; once enabled, a shared enroll secret can no longer enroll fleetd as a host enrolled in Fleet Windows MDM.

Enable per-device single-use Windows MDM enroll secrets to prevent a compromised shared secret from being reused across hosts.

yaml

```yaml
mdm:
  windows_one_time_enroll_secrets: true
```

— Config key, behaviour change, and example config shown `fleet-v4.94.0`

---

06 **WebSocket push for orbit-config updates** NEW

80

New experimental `websocket.orbit_config_enabled` setting (requires `websocket.transport_enabled`) pushes orbit-config change notifications over WebSocket instead of polling every 30 seconds, with `websocket.orbit_config_poll_interval` (default 5 minutes) and `websocket.orbit_config_spread` (default 30 seconds) controlling fallback polling.

— Full set of named settings and defaults, no example `fleet-v4.94.0`

---

07 **OpenTelemetry HTTP metrics switch to stable conventions**

80

BREAKING

OpenTelemetry HTTP server metrics for gorilla-routed requests now use stable semantic conventions: `http.server.request.duration` (seconds) replaces `http.server.duration` (milliseconds), and `http.server.request.body.size` / `http.server.response.body.size` replace `http.server.request.size` / `http.server.response.size`; custom dashboards built on the old metric names require updating.

— All metric names given with units, no migration command `fleet-v4.94.0`

---

08 **On-demand FileVault recovery key rotation** NEW 75

Admins can rotate a macOS host's FileVault recovery key on demand via API without waiting for the next scheduled escrow, e.g. `POST /api/v1/fleet/hosts/{id}/encryption_key/rotate`.

Rotate a macOS host's FileVault recovery key on demand without waiting for the next scheduled escrow.

```
$ curl -X POST
https://fleet.example.com/api/v1/fleet/hosts/42/encryption_key/ro
tate \
  -H 'Authorization: Bearer <token>'
```

— Runnable API call shown, limited mechanism detail `fleet-v4.94.0`

---

09 **Software type filter across software listing endpoints** NEW 73

Adds a `Types` filter via `source` and `extension_for` query parameters to the list software titles, list software versions, get host's software, and get device's software endpoints.

— Names all four endpoints and both query params `fleet-v4.94.0`

---

10 **Numeric version sort for OS versions endpoint** IMPROVED 70

Adds `version` as a valid `order_key` for `GET /api/v1/fleet/os_versions`, sorting by numeric version segment rather than lexical string order.

— Exact endpoint and parameter named `fleet-v4.94.0`

---

11 **GitOps file-reference support for maintained and App Store apps**

IMPROVED 68

Adds `path` / `paths` file-reference support to `software.fleet_maintained_apps` and `software.app_store_apps` in GitOps YAML, matching existing support for

`policies`, `labels`, `reports`, and `software.packages`.

— Names exact GitOps keys but no worked example `fleet-v4.94.0`

THINNER COVERAGE BELOW

12 **Hidden and self-service configuration profiles** NEW

55

Configuration profiles can now be marked `hidden` so they only appear on My device > Controls after the end user turns on the Show hidden profiles toggle, and macOS hosts support self-service configuration profiles that end users can install from the My device page.

— Describes behaviour and UI path, no example `fleet-v4.94.0`

13 **Renamed S3 software-installer signed-URL setting** DEPRECATED

55

The `s3_software_installers_signed_url` server option is renamed to `s3_software_installers_gcs_signed_url`; the old name still works but is deprecated.

— Names old and new keys but no migration steps `fleet-v4.94.0`

14 **GitOps profile rename now re-creates the profile** BREAKING

55

Renaming a Windows, Android, or declaration (DDM) profile through GitOps now re-creates the profile rather than updating it in place.

— States behaviour change but no detail on consequences `fleet-v4.94.0`

└──▷ **BREAKING ON UPGRADE**

! The `s3_software_installers_signed_url` server option is renamed to `s3_software_installers_gcs_signed_url`; the old name still works but is deprecated.

! OpenTelemetry HTTP server metrics for gorilla-routed requests now use stable semantic conventions: `http.server.request.duration` (seconds) replaces `http.server.duration` (milliseconds), and `http.server.request.body.size` / `http.server.response.body.size` replace `http.server.request.size` / `http.server.response.size`; any custom dashboards built on the old metric names require updating.

! When `mdm.windows_one_time_enroll_secrets` is enabled, a shared enroll secret can no longer enroll fleetd as a host that is enrolled in Fleet Windows MDM.

! Renaming a Windows, Android, or declaration (DDM) profile through GitOps now re-creates the profile.

WAS THIS USEFUL? 👍 👎

Iru

Feedback ⓘ New Windows Auto Apps NOTES ↗ RANK

Iru is a device-centric platform that unifies security, IT, and compliance around devices and everything they touch.

> Iru shipped Remote Shell for live root command-line access on managed Macs and added a GitHub Copilot Auto App to its macOS catalog.

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

01 Remote Shell for managed Macs NEW

75

Remote Shell gives a root command line on a managed Mac, reachable directly from a detection or the device record in the Iru console. It stays connected while a Mac is in Partial Isolation, allowing a threat to be contained and investigated at the same time.

Contain a suspected compromise and run live forensic commands on the Mac without losing shell access when Partial Isolation is applied.

> 📍 In the Iru console, open a detection or the device record, click Remote Shell, then run your investigation commands — Partial Isolation can be enabled on the same device without dropping the session.

— Describes mechanism, scope, and gives exact console steps Remote Shell

THINNER COVERAGE BELOW

02 GitHub Copilot macOS Auto App NEW SUPPORTED PLATFORM NEW

30

Iru adds a GitHub Copilot Auto App for macOS, now available to all customers via the Library Items catalog.

— Names the catalog location but no further detail New macOS Auto App: GitHub Copilot

New Windows Auto Apps NOTES ↗ STABLE

WAS THIS USEFUL? 👍 👎

Microsoft Intune

Feedback ⓘ Week of October 19, 2026

NOTES ↗ RANK

Microsoft Intune is a cloud-based unified endpoint management solution built on Zero Trust. Empower IT to manage, secure and govern devices, apps and endpoints.

> Microsoft Intune added support for unlimited-license assignment of Apple VPP apps.

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

01 **Unlimited licensing for Apple VPP apps** NEW 45

Intune now supports assigning Apple Volume Purchase Program apps with unlimited licenses sourced from Apple Business Manager and Apple School Manager on iOS/iPadOS and macOS, removing the need to track or manage license quantities.

— Clear description of behavior but no UI path or config detail. Week of October 19, 2026

WAS THIS USEFUL? 👍 👎

◆ Security Validation (BAS & Automated Pentest)

Datadog Stratus Red Team

Feedback ⓘ v2.37.2 NOTES ↗

CODE ↗

Granular, Actionable Adversary Emulation for the Cloud

└──▷ GET THIS VERSION ▾

Docker

```
$ docker pull ghcr.io/datadog/stratus-red-team:v2.37.2
```

Go

```
$ go install github.com/datadog/stratus-red-
team/v2/cmd/stratus@v2.37.2
```

git

```
$ git clone --branch v2.37.2 https://github.com/DataDog/stratus-red-
team.git
# already have the repo? check out this version:
$ git checkout v2.37.2
```

published under the project's GitHub account · Go module path matches the repo · checked 29 Oct

Wrong command?

NEW DETECTION EBS Volume Cross-Account Sharing Exfiltration Technique

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Backup & Recovery

Veeam Backup & Replication

Feedback ⓘ

changelog · Oct 29, 2026 CHANGELOG ↗ RANK

Veeam Backup & Replication is backup, recovery, and replication software for virtual, physical, cloud, and SaaS workloads.

> Veeam Backup & Replication adds support for VMware vCenter Server 9.1.1, removes compromised root CA certificates from its trust store, and updates several bundled third-party components.

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

01 **Compromised root CA certificates removed** IMPROVED 45

Removes compromised root CA certificates — the Comodo AAA Services root and affected emSign roots — from the trust store of the Veeam Software Appliance and Veeam components.

— Names exact certificates removed but no user action needed or given.

2026-10-29-dea3a0ab

02 **Third-party component updates** IMPROVED 35

Updates bundled third-party components including `OpenSSL 3.5.8`, `.NET runtime 10.0.12`, `PowerShell 7.6.6`, and Microsoft Edge WebView2.

— Lists exact versions but no behavioral or action detail. 2026-10-29-dea3a0ab

WAS THIS USEFUL? 👍 👎

◆ Non-Human & Agent Identity

Aembit

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗ RANK

Aembit is a runtime IAM for AI agents and workloads. Enforce access policies, keep downstream credentials out of agents, audit access, and revoke it with a kill switch.

> Aembit's MCP Identity Gateway gains a network access policy for restricting which MCP servers it can reach and exposes its version in unauthenticated metadata, alongside a batch of reliability and error-visibility fixes across Agent Controller and the gateway.

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

01 Gateway version in protected resource metadata NEW

68

The MCP Identity Gateway now exposes its version via the `aembit_gateway_version` field in the protected resource metadata document, which can be read without an access token.

— Names the exact field and auth-free access, but not the document's path

changelog-20261029-da919d95

02 Faster credential refresh after user-based token authorization

IMPROVED

65

MCP Identity Gateway now applies a new credential on the user's very next request after an MCP User-Based Access Token Credential Provider authorization, instead of returning errors until the cached credential expired.

— Clear before/after behavior change, no user action required changelog-20261029-da919d95

03 Network access policy for self-hosted MCP Identity Gateway

NEW

64

Aembit adds `AEMBIT_NETWORK_ACCESS_POLICY` to control which MCP servers a self-hosted MCP Identity Gateway can reach.

— Names the env var but not its accepted values or syntax changelog-20261029-da919d95

04 Tool-argument headers forwarded to earlier MCP spec clients

IMPROVED

60

MCP Identity Gateway now sends tool-argument request headers to MCP clients on earlier specification revisions when connecting to MCP servers on the 2026-07-28 MCP specification.

— Names the spec version but is a compatibility fix with no reader action

changelog-20261029-da919d95

THINNER COVERAGE BELOW

05 **Workload events record failed credential injection** IMPROVED

55

Workload events now record credential injection as failed when MCP Identity Gateway cannot add a credential to a request as a header or query parameter.

— Points reader to workload events for a concrete failure signal

changelog-20261029-da919d95

06 **Agent Controller bypasses proxy for AWS IMDS attestation**

IMPROVED

53

Agent Controller now bypasses an HTTP proxy when calling the AWS instance metadata service for AWS Metadata Service Trust Provider attestation, matching its existing Azure behavior.

— Clear before/after but automatic, nothing for reader to configure

changelog-20261029-da919d95

07 **Agent Controller auth errors name failing controller ID**

IMPROVED

50

Agent Controller authentication errors now name the Agent Controller ID that failed, prompting you to confirm it is valid and active in your Aembit Tenant.

— Gives a concrete troubleshooting step for the error changelog-20261029-da919d95

08 **Direct MCP server errors through tool access filtering**

IMPROVED

50

MCP clients now receive MCP server errors directly when MCP Tool Access Control is filtering a tool list and the upstream MCP server returns an error.

— Describes the behavior change but no mechanism detail changelog-20261029-da919d95

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

ConductorOne

Feedback ⓘ changelog · Oct 29, 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 introduced a user-scoped access review type, restructured access profiles into three distinct behaviors, and launched a consolidated Browse page for requestable access.

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

01 Catalog, Role, and Hybrid access profile types NEW

88

Access profiles now come in three types: Catalog (self-service requestable), Role (automatic all-or-nothing grants based on explicit membership), and Hybrid (the prior behavior — requestable or condition-based). All existing profiles are automatically converted to Hybrid. To create a Role profile, go to Access Profiles > New Profile, select Role, define the membership condition, and save; membership can then be granted, revoked, or requested like any other entitlement.

Convert a new access profile to a Role profile so that access is granted automatically and all-or-nothing based on membership, rather than being self-service requestable.

> 📍 In ConductorOne, go to Access Profiles › New Profile, when prompted select the Role type, define the membership condition, and save; membership can then be granted, revoked, or requested like any other entitlement.

— Names all three types, migration behavior, and exact creation steps

changelog-20261029-ec98f2aa

THINNER COVERAGE BELOW

02 Browse page for requestable access NEW

48

A new Browse page consolidates everything a user can request in one place, including a dedicated AI tools tab, while the Requests page is now limited to task queues only.

— Describes the change but no detailed navigation or config changelog-20261029-ec98f2aa

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Nudge Security

Feedback ⓘ changelog · Oct 29, 2026

CHANGELOG ↗

Nudge Security is a SaaS security platform that discovers shadow IT assets, manages identity governance, and hardens security posture.

Nudge Security now blocks nudges to deleted, archived, or suspended users, and bulk sends report skipped recipients.

Nudge Security now blocks sending nudges to deleted, archived, or suspended users and accounts, with the nudge button disabled and a message explaining why delivery is not possible.

Bulk nudge sends now report which recipients were skipped due to deleted, archived, or suspended status.

NEW INTEGRATION Notion AI agent discovery

WAS THIS USEFUL? 👍 👎

Ping Identity

Feedback ⓘ changelog · Oct 29, 2026 CHANGELOG ↗

RANK

Ping Identity is an identity and access management platform providing authentication, single sign-on, multi-factor authentication, and identity governance services.

> Ping Identity's latest Advanced Identity Cloud changelog introduces an opt-in Remote MCP Server for AI-agent administration, adds QR code callbacks and multi-alias SAML IdP import, and tightens enum-value normalization in a way that can break existing scripts.

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

01 **Multi-alias SAML IdP import** NEW 85

You can now import multiple remote identity providers that share the same entity ID by specifying an alias, with uniqueness enforced per circle of trust. Aliased providers do not support single logout or Enhanced Client or Proxy (ECP), and hosted service-provider assertion consumer service URLs require a manual `cot` parameter.

— Full mechanism, limitations and parameter named changelog-20261029-07d5f16d

02 **Issuer verification in OIDC responses** IMPROVED 75

The OpenID Connect discovery endpoint now always returns `authorization_response_iss_parameter_supported: true`, and authorization responses (including error responses) now include the `iss` parameter so clients can verify the response issuer.

— Exact field names given, directly verifiable changelog-20261029-07d5f16d

03 **AIC Remote MCP Server for AI agents** NEW 70

A new opt-in, centrally hosted HTTP-based Model Context Protocol server lets AI agents and development assistants administer Advanced Identity Cloud via natural-language prompts over OAuth 2.0 authentication. It is available now in sandbox environments.

— Names protocol and auth method but no endpoint or setup steps

changelog-20261029-07d5f16d

04 **Case-insensitive enum matching with schema normalization** 70

BREAKING

Managed object enum-typed properties are now matched and rewritten without regard to case, normalizing submitted values to the exact case defined in the schema. This is a breaking change: scripts or dashboards that compare `accountStatus` or other enum

property values against non-canonical cases (e.g. `Active` instead of `active`) must be updated to expect the schema-defined case.

— Clear migration note but no specific config key listed `changelog-20261029-07d5f16d`

05 **QR code callback for scripted nodes** NEW 65

A new callbacksBuilder.qrCodeCallback() binding for scripted nodes lets them generate QR codes that render in hosted pages or apps built with the Ping SDKs.

— Exact method name given, no further config detail `changelog-20261029-07d5f16d`

06 **Reporting improvements for optional parameters and reviewer field**

IMPROVED 60

Several parameters in built-in reports are now optional, allowing reports to run with broader criteria, and in custom reports the `Completed By` field in the `Entitlement Review Item` entity now returns the `userName` value.

— Names exact field but not which parameters became optional `changelog-20261029-07d5f16d`

THINNER COVERAGE BELOW

07 **Custom name formats for WS-Fed SP attributes** IMPROVED 45

Custom WS-Fed applications now support user-defined name formats for service provider attributes, letting you specify custom namespaces to meet the attribute requirements of specific relying parties.

— Describes capability but no config key or UI path `changelog-20261029-07d5f16d`

08 **Larger Identity Governance workflow definitions** IMPROVED 40

Identity Governance now accepts workflow definitions up to 1 MiB.

— Single size limit, no further mechanism described `changelog-20261029-07d5f16d`

09 **Delegated admins view own relationship properties** NEW 40

Delegated administrators can now view their own relationship properties in the hosted account pages.

— UI path given but no further detail `changelog-20261029-07d5f16d`

10 **Unique usernames and application names enforced** IMPROVED 30

The underlying datastore now enforces unique usernames and application names.

— Thin description with no migration guidance changelog-20261029-07d5f16d

└──▷ **BREAKING ON UPGRADE**

! Managed object enum values are now normalized to schema-defined case on write — scripts or dashboards that compare `accountStatus` or other enum property values against non-canonical cases (e.g. `Active` instead of `active`) must be updated to expect the exact case defined in the schema.

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ Release Notes 2026 (2026-10-28) BLOG ↗

RANK

JumpCloud makes it simple to manage Windows, Apple, Linux, and Android devices and to deliver secure access with SSO, MFA, Zero Trust, RADIUS, and more.

> JumpCloud's October 2026 release adds a SIEM integration for Directory Insights, Agent Uninstall Protection, new REST APIs for AI agent identities, an MCP Server for Users, Custom Risk Policies, and several smaller User Portal and MDM privacy additions.

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

01 **Agent Uninstall Protection for devices** NEW 95

Protects against unauthorized agent removal, on by default for devices running JumpCloud agent v2.179.2 or later, and requires a per-device maintenance token to uninstall on macOS, Windows, and Linux. Manage it at `Device Management > Devices > Settings > Agent Uninstall Protection` and use the Disable Agent Uninstall Protection policy to exempt specific devices.

Exempt a device from Agent Uninstall Protection during imaging or maintenance without requiring a maintenance token.

> 📍 Go to Device Management › Devices › Settings › Agent Uninstall Protection, then assign the Disable Agent Uninstall Protection policy to the target device or device group.

— Exact version threshold, UI path, and policy name given Release Notes 2026 (2026-10-28)

02 **SIEM integration for Directory Insights** NEW 80

Continuously pull JumpCloud identity events into external SIEM platforms using an existing API key, with support for RAW and OCSF-normalized formats. Admins can also run asynchronous historical export jobs covering up to 7-day windows across a 13-month retention lookback, delivered as JSON or CSV files with email notification on completion.

— Mechanism and limits named, but no exact API path given Release Notes 2026 (2026-10-28)

03 **MCP Server for Users** NEW 75

Connect AI clients directly to User Portal capabilities via the new JumpCloud MCP Server for Users, using OAuth sessions. Admins enable it at `Settings > JumpCloud AI`, and users manage their own sessions at `Security > JumpCloud MCP` in the User Portal.

Enable the MCP Server for Users so staff can perform User Portal tasks from their AI clients without switching tools.

> 📍 Go to Settings › JumpCloud AI and toggle on MCP Server for Users. Users can then view and revoke their own active sessions at Security › JumpCloud MCP in the User Portal.

— Exact enable and session-management paths given Release Notes 2026 (2026-10-28)

---

04 **REST APIs for AI agent identities** NEW 70

New Agents API and Agent Groups API let admins register, retrieve, update, suspend, activate, and delete agent identities, manage their credentials, manage agent groups, and control group memberships and application assignments.

— Named APIs and operations, but no endpoint paths given Release Notes 2026 (2026-10-28)

---

05 **Custom Risk Policies for logins** NEW 70

Tailor risk detection for Admin Portal, User Portal, device, and SSO application logins, setting per-user-group or per-application rules, choosing risk factors, adjusting score contributions, and controlling policy precedence.

— Scope and controls described, but no config path given Release Notes 2026 (2026-10-28)

---

06 **App Settings Privacy policies for Apple MDM** NEW 70

Apply App Settings Privacy policies to recommend privacy permission defaults for applications on supervised macOS 27, iOS 27, or iPadOS 27 or later devices, covering permissions including Accessibility, Bluetooth, Camera, Dictation, Local Network, Location, and Microphone.

— OS versions and permission list named, no UI path given Release Notes 2026 (2026-10-28)

---

07 **Custom Messaging in User Portal** NEW 60

Create login dialogs and announcement banners for User Portal users, scoped by user group and severity. Available at `Settings > User Portal > Custom Messaging`.

— Exact settings path given but scope mechanism is thin Release Notes 2026 (2026-10-28)

THINNER COVERAGE BELOW

---

08 **User Portal application folders and asset visibility** NEW 55

End users can organize assigned applications into personal folders on the User Portal's `All Applications > Folders` tab, and can view their assigned assets with admins able to request acknowledgement on assignment or reassignment, enabled at `Device Management > Asset Management > Settings and Fields > General Settings`.

— Two thin User Portal additions, each with an exact path Release Notes 2026 (2026-10-28)

09 **Custom Banned Password List** NEW 30

Block specific words, terms, and phrases from user passwords, configured in Password Policies.

— Only a one-line description with no exact path Release Notes 2026 (2026-10-28)

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Auth0 Feedback ⓘ

Introducing Universal Portals - Developer Preview (2026-10-27) BLOG ↗ RANK

Secure users, AI agents, and more with Auth0, an easy-to-implement, scalable, and adaptable authentication and authorization platform.

> Auth0 introduced Universal Portals in Developer Preview — hosted, self-service portals for end users and organization admins, built with a visual page builder and Auth0 Forms, backed by server-side token handling and automatic MFA step-up.

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

01 Visual portal builder with Universal Components and Auth0 Forms

NEW 75

Portal pages are built visually using Universal Components, Auth0 Forms, and layout components such as headings, rich text, sections, separators, and images. An Auth0 Form can be added to any portal page to collect or update information, including profile updates, policy acceptance, and communication preferences.

Embed an Auth0 Form on a portal page to collect policy acceptance from users on login.

📍 In the Auth0 dashboard, go to Customize › Portals, open a portal page in the visual builder, select Add Component › Auth0 Form, choose your policy-acceptance Form, and save.

— Names concrete builder components and an exact dashboard workflow for adding a form.

Introducing Universal Portals - Develop…

02 Consumer and business self-service portals NEW 60

Auth0 now offers hosted consumer portals where end users can update their profile, enroll MFA factors and passkeys, and review security settings — served on your domain with no interface to build or maintain. It also offers business portals where organization administrators can edit organization details and verify domains, without custom development.

Set up a consumer portal so end users can self-serve MFA enrollment and profile updates without you building any UI.

📍 In the Auth0 dashboard, go to Customize › Portals, create a new portal of type Consumer, add a Universal Component for MFA enrollment, and publish it to your

tenant domain.

— Names both portal types and their capabilities but little mechanism beyond hosting.

Introducing Universal Portals - Develop…

THINNER COVERAGE BELOW

03 **Automatic MFA step-up challenge in portals** NEW 45

Portals automatically trigger an MFA step-up challenge when Auth0 requires MFA for an operation, then retry the operation once the user completes it.

— Describes trigger-and-retry behavior but no setup or configuration steps.

Introducing Universal Portals - Develop…

04 **Server-side token storage for portal sessions** NEW 40

Portal servers hold access and refresh tokens server-side; the browser receives only a secure session cookie, so tokens never reach client-side code.

— Explains the security mechanism but offers no configuration detail.

Introducing Universal Portals - Develop…

05 **Portal branding inheritance** NEW 35

Portals inherit your tenant's logo, colors, and fonts by default, or switch to an organization's branding when the portal is opened in an organization context.

— Describes behavior but gives no configuration path or control.

Introducing Universal Portals - Develop…

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL?

RIG Security

Feedback ⓘ Your AI Agent Is Wearing Your Badge

NOTES ↗ RANK

Rig security is a rig ties every account, token, and AI agent to the human behind it. Map attack paths, enforce least privilege, and detect identity threats in one platform.

> RIG Security launched Gatewatch, an endpoint agent that attributes cloud actions to the human or AI agent actually driving them and can block policy violations before they reach the cloud.

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

01 **Gatewatch endpoint agent for AI identity attribution** NEW

62

Gatewatch distinguishes between a human typing a command and an AI coding agent (such as Claude Code, Cursor, or Copilot) spawning the same command by following the full process tree at the endpoint. It evaluates policies in real time at the endpoint — before a request reaches AWS, Kubernetes, or other cloud targets — allowing or blocking actions based on the combination of process, identity, and action. Coverage extends to AI coding agents, CLI agents, and local MCP servers running on an engineer's machine with the engineer's credentials, where borrowed-identity risk originates.

— Explains mechanism and scope but no config/CLI/API surface given.

Your AI Agent Is Wearing Your Badge

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

Knocknoc

Feedback ⓘ v26.10 NOTES ↗ RANK

> Knocknoc's v26.10 release adds Trust Engine risk scoring via Spur and IPinfo, native SIEM forwarding to Splunk, Splunk Cloud, Cribl and Microsoft Sentinel, and broad device integration improvements, alongside predefined network management, an agent IPFilter integration, a new system health dashboard, richer audit logging, and tighter admin session controls.

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

01 Device integration expansion and reliability IMPROVED

85

Generates Palo Alto and Panorama device API keys directly within the Knocknoc setup workflow; processes access changes independently per device so a slow or unreachable firewall no longer holds up grants on healthy devices; adds network-range grant support across MikroTik, SonicWall, Sophos, Cisco Firepower, Azure, Cloudflare, Fortinet, nftables, and ipset; improves batching for F5 and Cloudflare to reduce repetitive device writes during bursts of access activity; and moves pfSense to network-compatible alias types for new configurations while existing configurations continue working.

— Names every affected device vendor and the pfSense migration note v26.10

02 Threat intelligence risk scoring via Trust Engine NEW

75

Adds Spur and IPinfo threat intelligence integrations to the Trust Engine to assess connection risk — including residential proxies, commercial VPNs, and Tor exit nodes — after authentication but before network access opens, with support for BYOK (bring-your-own credentials) or Knocknoc-provided options.

— Names providers and BYOK option but no config key given v26.10

03 Structured action logging and SIEM integrations NEW

75

Knocknoc now writes a structured log line for every notable action and forwards them to configured destinations; this now includes sending security and access events directly to Splunk, Splunk Cloud, Cribl, and Microsoft Sentinel without additional log collectors or storage pipelines, supporting multiple simultaneous destinations and a new SIEM integration view showing delivery status and failure details.

— Names four SIEM destinations and a status view, no exact endpoint v26.10

04 **Unified agent and system health dashboard** NEW 60

Adds a unified view of system and orchestration agent health — including certificate, licensing, threat-intelligence, agent compatibility, and server consistency issues — with historical performance data and links to troubleshooting guidance, and lets users save frequently used portal views and personalise layouts.

— Lists monitored issue types and a saved-views feature with no exact path v26.10

THINNER COVERAGE BELOW

05 **Predefined networks for configuration reuse** IMPROVED 55

Predefined networks are named lists of networks defined once and reused across multiple places in configuration, including access configurations and security policies. Controls let administrators decide whether active access ends immediately or expires naturally when a network range is removed, and users can select specific network sources rather than opening access to all available sources where predefined networks allow it.

— Describes lifecycle controls but no config key or UI path v26.10

06 **Administrator session and sign-in controls** NEW 45

Adds the ability to terminate administrator sessions on demand, in addition to the existing user-session termination feature, restricts where administrators can sign in, and applies smarter protection against account lockouts.

— Names the capability but not the sign-in restriction mechanism v26.10

07 **Richer configuration and session audit logging** IMPROVED 40

The configuration audit log now captures richer before-and-after change information, and sessions can be followed into the audit log with exportable identity and session detail.

— Describes the change but names no field or export format v26.10

08 **IPFilter host network control** NEW 35

Knocknoc's agent now integrates with IPFilter to dynamically control network access on the host it runs on.

— Names the integration but gives no setup or usage detail product docs

WAS THIS USEFUL?  

Cato Networks

Feedback ⓘ

See the Real AI Experience with Cato DEM (2026-10-29) BLOG ↗

Cato networks is a cato SASE Cloud converges SD-WAN, security, global backbone, and remote access into a global cloud-native service. WE ARE SASE™

Cato DEM adds AI Agent Experience Monitoring with a dedicated drill-down for AI latency and errors by model provider, domain, site, and access method.

Cato DEM now adds an AI Agent Experience Monitoring drill-down view where IT teams can analyze AI latency and errors broken down by model provider, domain, and site.

NEW INTEGRATION Cato DEM now isolates AI model-provider traffic — including conversational interactions and coding-agent traffic from tools like Claude Code — from background application noise such as downloads, authentication, and telemetry, so latency and error metrics reflect the actual AI interaction.

Cato DEM now shows how users are accessing AI services — browser, terminal, script, or coding tool — so IT can distinguish, for example, a browser session to Claude from a developer using Claude Code.

WAS THIS USEFUL? 👍 👎

DNSFilter

Feedback ⓘ

10/28 October 28 – Web Application and API Update (2026-10-28) BLOG ↗ RANK

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

> DNSFilter expanded block page localization to eight more languages and documented a new API call to restart failed data exports without re-entering SIEM credentials.

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

01 **Unblock request form localization expanded** IMPROVED

55

The block page unblock request form now displays in Italian, Dutch, Portuguese, Russian, Swedish, Czech, Turkish, and Ukrainian based on the user's browser language setting, joining existing support for Spanish, French, and German.

— Names all languages but no config or setup steps

10/28 October 28 – Web Application and …

02 **API call to restart failed data export** NEW

50

DNSFilter's API documentation now includes the call to restart a failed Data Export using saved connection settings, so no SIEM credentials are needed to retry.

— Describes behavior but no endpoint name or method given

10/28 October 28 – Web Application and …

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

cryptomator

Feedback ⓘ 1.19.5 NOTES ↗ RANK

Cryptomator for Windows, macOS, and Linux: Secure client-side encryption for your cloud storage, ensuring privacy and control over your data.

> Cryptomator 1.19.5 broadens supporter-certificate validation and hardens masterkey handling against excessive scrypt memory parameters, alongside a usability tweak to the trust-on-first-use dialog.

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

01 **Masterkey scrypt parameter validation** IMPROVED 70

Masterkey files whose scrypt parameters would require more than 64 MiB of memory are now rejected before key derivation, with a dedicated error dialog shown on unlock and password change.

– Explains mechanism, threshold and when the dialog appears 1.19.5

THINNER COVERAGE BELOW

02 **Certificate-chain support for supporter certificates** NEW 50

Cryptomator now accepts supporter certificates signed via a certificate chain using the `x5c` header, broadening the set of valid certificate formats.

– Names the x5c mechanism but no usage steps 1.19.5

03 **Trust-on-first-use dialog usability** IMPROVED 20

Cryptomator improves usability of the trust-on-first-use dialog.

– Bare description with no specifics on the change 1.19.5

WAS THIS USEFUL? 👍 👎

◆ Public Key Infrastructure (PKI)

lego

Feedback ⓘ v5.6.0 NOTES ↗ RANK

Let's Encrypt/ACME client and library written in Go

> lego v5.6.0 expands DNS provider coverage with six new providers and adds a compatibility fix for Google Trust Services in the dns-persist-01 challenge.

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

01 **Six new DNS providers for dns-01 challenges** NEW 55

lego adds DNS providers for `CloudPress`, `GoDaddy v3`, `Netcup v1`, `NordName`, `PrimeDNS`, and `Selfhost v2`, enabling ACME dns-01 challenge automation against zones hosted on each of these services; Selfhost v2 specifically supports the updated Selfhost API.

– Names all six providers but no config/flag detail v5.6.0

02 **Google Trust Services workaround in dns-persist-01** IMPROVED 30

lego's `dns-persist-01` challenge now includes a workaround for Google Trust Services compatibility.

– Names the challenge and CA but no mechanism detail v5.6.0

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Compliance Automation & Trust Management

Compyl

Feedback ⓘ Oct 27th, 2026 NOTES ↗

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

NEW INTEGRATION Workspace ONE integration

NEW INTEGRATION Supabase integration

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI Red Teaming & Testing

AI-Infra-Guard

Feedback ⓘ v4.6.8 NOTES ↗ RANK

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

> AI-Infra-Guard made each scanner independently installable via pip and added a Runcrate provider preset to Agent-Scan, broadening the agent runtimes it can target.

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

01 **Independent pip install per scanner** IMPROVED 55

Each scanner in the suite can now be installed on its own via `pip install` without pulling in the full tool, letting users adopt a single scanner in isolation.

— Names the pip install mechanism but no package names given v4.6.8

02 **Runcrate provider preset in Agent-Scan** NEW 40

Agent-Scan now supports Runcrate as a provider preset, expanding the range of agent runtimes it can target.

— Names the feature and target but no usage steps given v4.6.8

WAS THIS USEFUL? 👍 👎

◆ AI/LLM Security

ToolHive

Feedback ⓘ v0.59.0 NOTES ↗ RANK

ToolHive is an enterprise-grade platform for running and managing Model Context Protocol (MCP) servers.

> ToolHive's v0.59.0 release focuses on securing operator-managed infrastructure and deepening OAuth/MCP client support, adding TLS for Redis defaults, a Windows credential helper for Claude Desktop, and several OAuth/DCR refinements.

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

01 **Live re-checking of upstream DCR registrations** IMPROVED 50

ToolHive re-checks upstream Dynamic Client Registration (DCR) registrations while servers are running, keeping registrations current without requiring restarts.

– Describes mechanism and benefit but no config surface named v0.59.0

02 **Windows Claude Desktop credential helper** NEW 45

ToolHive adds a credential helper for Windows Claude Desktop, extending client integration to Windows users.

– Clear capability but no command or install path given v0.59.0

03 **TLS for operator-wide Redis defaults** IMPROVED 40

ToolHive now supports enabling TLS for operator-wide Redis defaults, securing broker connections in Kubernetes deployments.

– Names Redis/TLS/Kubernetes but no config key or flag given v0.59.0

04 **In-memory backend for exchange grant data** NEW 40

ToolHive adds in-memory backend storage for exchange grant data, supporting OAuth token exchange workflows.

– Names storage type and purpose but no API or flag v0.59.0

05 **Context7 integration ownership and library config** IMPROVED 40

ToolHive adds Context7 ownership verification and expanded library configuration for the Context7 integration.

– Names integration and two additions but no specifics v0.59.0

06 **Configured delegate client metadata support** NEW 30

ToolHive adds configured delegate client metadata support to expand OAuth delegation capabilities.

— Thin description with no concrete fields or config named v0.59.0

WAS THIS USEFUL? 👍 👎

Straiker Feedback ⓘ

Straiker Brings Independent AI Agent Red-Teaming to Workday (2026-10-16) BLOG ↗

RANK

Straiker discovers and inventories enterprise AI agents, tests them with automated red teaming and protects them with runtime guardrails.

> Straiker now integrates with Workday Agent Passport, letting its Ascend AI red-team assessments feed a new independent trust category for AI agents before enterprises install them.

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

01 **Workday Agent Passport red-team integration** NEW 68

Straiker added an integration with Workday Agent Passport that submits signed Ascend AI red-team assessment results through Workday's partner interfaces, giving agents verifiable evidence of adversarial testing tied cryptographically to the specific agent version tested before customers install them. Ascend AI now probes agents against Workday-defined Stamps — including Prompt Injection Resistance — covering attack paths from the OWASP LLM Top 10, the OWASP Agentic Security Initiative, and MITRE ATLAS. This powers a new Adversarial Resilience Trust Category in Workday Agent Passport, sourced from independent partners such as Straiker, joining six existing categories: Build Integrity, Runtime Safety, Audit Integrity, Data Sovereignty, Delegated Authority & Human Control, and AI Governance.

— Names integration, standards covered, and trust category, but no API/flag to act on.

Straiker Brings Independent AI Agent Re…

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

joplin

Feedback ⓘ v3.7.22 NOTES ↗ RANK

Joplin - the privacy-focused note taking app with sync capabilities for Windows, macOS, Linux, Android and iOS.

> Joplin's v3.7.22 release expands its MCP tooling with a new note-reading tool and richer search context, and adjusts how private-network AI providers are treated for trust purposes.

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

01 **MCP note reading and search context tools** NEW 60

Joplin adds a `read_notes` MCP tool for reading notes via the Model Context Protocol, using outline and section navigation to reduce token consumption. The existing `search_notes` MCP tool now also returns the enclosing section alongside each result.

— Names MCP tools but no usage example or exact invocation shown v3.7.22

THINNER COVERAGE BELOW

02 **Private network AI providers treated as local** IMPROVED 30

AI providers reachable on private networks are now treated as local for connectivity and trust purposes.

— Brief behavior note with no mechanism or config detail v3.7.22

WAS THIS USEFUL? 👍 👎

INFRASTRUCTURE

◆ Internet Services

Cloudflare

Feedback ⓘ

China Network, Challenges, Bots - China-native Challenge Pages for the China Network (202

BLOG ↗ RANK

Cloudflare is a connectivity cloud platform delivering internet security, performance, and developer infrastructure services.

> Cloudflare's China Network now serves Turnstile challenge widgets from servers hosted inside Mainland China, removing cross-border requests for visitors there.

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

01 **China-hosted Turnstile challenge widgets** IMPROVED 40

Challenge Pages on the China Network now use Turnstile widgets hosted in Mainland China, so visitors there complete challenges faster and more reliably without cross-border requests. No configuration change is required to benefit.

— Explains behavior change but no config, metrics, or rollout detail.

China Network, Challenges, Bots - China…

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 29, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue