THE CYBER TOOLCHAIN

NO. 144

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED NOVEMBER 19, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 221 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 66 of 67 tools

▾ // THE BRIEF

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

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

Three unrelated things stand out today: StepSecurity can now put a blocking layer in front of JavaScript installs in CI, Veracode added

vim ? help

repository-wide package blocking, and JumpCloud can turn access-review decisions into actual revocations instead of tickets.

PROTECT

Block risky packages before they land in builds

StepSecurity's Secure Registry routes npm, npx, pnpm, and Bun installs through a layer that blocks malicious packages and delays new releases; Veracode's Package Firewall blocks untrusted packages across repositories. That moves dependency defense from after-the-fact scanning toward preventing a bad package from entering the build path at all.

StepSecurity · Veracode

GOVERN

Make access certifications enforce themselves

JumpCloud now automates access revocation and suspension when certification decisions are finalized or deadlines expire, and adds tamper-proof certification exports. Review outcomes no longer have to become manual follow-up work before they reduce access.

JumpCloud

DETECT

Add ready-made detections for current attack techniques

Splunk Security Content added 17 detections and 3 analytic stories across Java deserialization, Linux service-account abuse, browser cache smuggling, command-line evasion, and C2 tunneling; AI DFIR Toolkit added Sigma rules for Entra app abuse and SSH tunnels plus downloadable IOC feeds. Teams get more coverage they can adapt instead of starting each hunt from scratch.

Splunk Security Content · AI DFIR Toolkit

PROTECT

Reduce accidental host exposure from sandboxed workloads

minimal replaced its single host-port exposure environment variable with a live-reloading `[host-exposures]` table in `config.toml`. Operators can narrow which host ports boxes may reach without restarting everything, reducing the chance that a convenience exposure becomes a standing escape path.

minimal

Does **GPT-5.5** read better? 👍 👎

OFFENSIVE SECURITY

◆ Exploitation & C2

BC Security powershell-empire

Feedback ⓘ v7.1.0

NOTES ↗ RANK

Powershell-empire is an empire is a post-exploitation and adversary emulation framework that is used to aid Red Teams and Penetration Testers.

> Empire 7.1.0 adds container-friendly file logging with rotation controls and listener support for a separate public port behind reverse proxies, alongside a major hardening of the agent communication protocol (handshake-signed Ed25519 signatures, HKDF-derived AES/HMAC keys) and a string of breaking changes to listeners, stagers, module file options, and the OpenAPI schema.

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

01 File logging with rotation controls

Not checked yet NEW

95

Empire now supports file logging with rotation when run in containers, controlled via `logging.file_logging`, `logging.max_bytes`, and `logging.backup_count` in server config, or the `EMPIRE_LOGGING__FILE_LOGGING` environment variable. `empire_server.log` and `listener_<name>.log` rotate by default at 10 MB with 5 backups; set `logging.max_bytes: 0` for unbounded logs.

Run Empire in a container with log output going only to the console, or enable file logging with rotation limits so logs do not grow unbounded.

yaml

```yaml
logging:
  file_logging: true
  max_bytes: 10485760
  backup_count: 5
```

Suppress file logging entirely via environment variable when deploying Empire as a container where stdout is captured by the orchestrator.

```
$ EMPIRE_LOGGING__FILE_LOGGING=false empire-server
```

— Full config keys, env var and defaults with runnable examples v7.1.0

02 Agent protocol crypto hardening

Not checked yet BREAKING

80

STAGE1 Ed25519 signatures now cover the full handshake transcript instead of the constant `"SIGNATURE"`, and the AES-CBC payload layer derives separate AES and HMAC keys from the shared key via HKDF-SHA256 (`empire-enc` / `empire-mac`) instead of reusing one key. Both changes break compatibility with pre-7.1 agents and existing sessions, so agents must be re-staged.

— Clear mechanism and before/after with migration note v7.1.0

---

03 **Listener and stager default behavior changes** Not checked yet

78

BREAKING

The `linux/pyinstaller` stager's `BinaryFile` option is now a bare file name defaulting to `empire` rather than `/tmp/empire`, with any directory component ignored. The `http` and `http_malleable` listeners now serve their configured default response instead of a Werkzeug 500 page for any error that escapes a view. The `http_hop` listener's `OutFolder` is now relative to `downloads/http_hop` and defaults to `redirectors`; hop listeners stored with an absolute path outside it no longer start.

— Names each option and its new default across three surfaces v7.1.0

---

04 **OpenAPI operation id and tag restructuring** Not checked yet

73

BREAKING

OpenAPI operation ids are now `{tag}_{route name}` (e.g. `agents_read_agent`) instead of FastAPI's path-and-method default, renaming the three generated `Body_*` request schemas, so every generated client method name changes. Agent-task and plugin-task routes are now tagged with only their primary resource, dropping the `tasks` tag group, and the `/api/v2/obfuscation` routes moved from the `keywords` tag to `obfuscation`.

— Names exact operation id pattern, tags and routes affected v7.1.0

---

05 **Module file options restricted to downloads directory**

Not checked yet

62

BREAKING

The `ExtFile`, `File`, and `Shellcode` module options must now name a path inside the server's downloads directory; saved workflows pointing elsewhere are rejected until the file is uploaded through the API.

— Names exact options and new constraint, no example given v7.1.0

THINNER COVERAGE BELOW

---

06 **Separate public port for listeners behind reverse proxies**

Not checked yet NEW

30

Listeners can now advertise a separate public port for reverse-proxy deployments, so the externally visible port can differ from the port the listener actually binds to.

— No config key or flag named, mechanism unclear `v7.1.0`

└──▷ BREAKING ON UPGRADE

! STAGE1 Ed25519 signatures now cover the handshake transcript instead of the constant `"SIGNATURE"`; re-stage all pre-7.1 agents or they will fail to connect.

! The AES-CBC payload layer now derives separate AES and HMAC keys from the shared key with HKDF-SHA256 (`empire-enc` / `empire-mac`) instead of reusing one key; existing sessions are incompatible.

! The `linux/pyinstaller` stager's `BinaryFile` option is now a bare file name defaulting to `empire` rather than `/tmp/empire`; any directory component is ignored.

! The `http` and `http_malleable` listeners now serve their default response instead of a Werkzeug 500 page for any error that escapes a view.

! The `http_hop` listener's `OutFolder` is now relative to `downloads/http_hop` and defaults to `redirectors`; hop listeners stored with an absolute path outside it no longer start.

! OpenAPI operation ids are now `{tag}_{route name}` (e.g. `agents_read_agent`) instead of FastAPI's path-and-method default, renaming the three generated `Body_*` request schemas; every generated client method name changes.

! The agent-task and plugin-task routes are now tagged with only their primary resource, dropping the `tasks` tag group.

! The `/api/v2/obfuscation` routes moved from the `keywords` tag to `obfuscation`.

! `empire_server.log` and `listener_<name>.log` now rotate at 10 MB with 5 backups, deleting older data; set `logging.max_bytes: 0` for unbounded logs.

! The `ExtFile`, `File`, and `Shellcode` module options must now name a path inside the server's downloads directory; saved workflows pointing elsewhere are rejected until the file is uploaded through the API.

WAS THIS USEFUL? 👍 👎

BC Security Starkiller

Feedback ⓘ v4.1.0 NOTES ↗

RANK

Starkiller is a Frontend for Empire.

> Starkiller v4.1.0 restores several agent terminal commands that had been removed with the Empire CLI, letting operators manage agents directly without leaving the terminal.

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

01 **Restored agent terminal commands** Not checked yet NEW

75

The agent terminal now supports `download`, `kill_date`, `working_hours`, `kill_job`, `kill`, and `rename` commands, restoring verbs that were previously removed from the Empire CLI. `kill` and `rename` update the agent list immediately without requiring a manual refetch.

Terminate a running agent job and schedule a kill date without leaving the agent terminal.

> 📍 In the agent terminal, type `kill_job` to stop a specific job, or `kill_date` to set a future termination time, or `kill` to task the agent to exit — the agent list updates immediately without a manual refetch.

— Names exact commands and behavior, but lacks deeper mechanism detail. v4.1.0

WAS THIS USEFUL? 👍 👎

NetSPI OCInferno

Feedback ⓘ changes since 2026-11-18 CODE ↗

OCInferno adds a `points_to` column to the Network Inventory report and now matches `--exclude-node` against display names as well as node IDs

Attack path exclusions via `--exclude-node` now match against a node's display name in addition to its internal ID, so human-readable labels can be used to exclude nodes.

Not checked yet

WAS THIS USEFUL? 👍 👎

Infobyte isr-evilgrade

Feedback ⓘ v3.0.0 CODE ↗

RANK

Isr-evilgrade is an evilgrade is a modular framework that allows the user to take advantage of poor upgrade implementations by injecting fake updates.

> isr-evilgrade v3.0.0 ships a Docker-based deployment path with automated DNS/MITM setup, new MITM interception modules for git clone and curl|sh installer vectors, SSL certificate and recursive-loader improvements to the update-chain modules, a SolarWinds Orion interception module, and a bulk Perl script to generate modules for the full CVE database.

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

01 **Docker-based deployment with automated MITM setup** Not checked yet

NEW 90

Adds a `docker-setup.sh` script and `docker-compose.yml` to run evilgrade in a container with automated DNS and MITM configuration, exposing ports 80, 443, 8080, and 8443.

Run the container directly with the required network capabilities and bind all interception ports to the host

```
$ docker run -it --rm \
  --name evilgrade-pentest \
  --cap-add=NET_ADMIN \
  --cap-add=NET_RAW \
  -p 80:80 -p 443:443 -p 8080:8080 -p 8443:8443 \
  -v $(pwd):/evilgrade \
  evilgrade:latest
```

— Names exact script, compose file, ports; runnable docker command given. v3.0.0

02 **Bulk module generation for full CVE database** Not checked yet

NEW 65

A `generate_all_modules.pl` Perl script bulk-generates interception modules for the full CVE database in one pass.

Bulk-generate Perl interception modules for the full CVE database in one pass

```
$ perl generate_all_modules.pl
```

— Names exact script and gives a runnable command to run it. v3.0.0

THINNER COVERAGE BELOW

03 **New MITM modules for git clone and curl|sh installer vectors**

Not checked yet NEW 55

Adds a `git clone` MITM module that serves a trojanized payload and a `curl|sh` installer MITM module targeting the eMudhra CA vector.

— Names two modules and their targets but gives no flags or commands. v3.0.0

04 **SSL certificate support and recursive loader for update-chain modules**

Not checked yet IMPROVED 35

Adds selectable SSL certificate support and a recursive loader to the update-chain module set.

— Describes the addition but gives no concrete config or usage. v3.0.0

05 **SolarWinds Orion update-interception module** Not checked yet NEW 20

Adds a module for intercepting SolarWinds Orion update requests, per the release summary; no further implementation detail is provided.

— Only named in the summary, with no mechanism or usage detail. v3.0.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Secrets Detection & Management

GitGuardian Self-Hosted

Feedback ⓘ

changelog · Nov 19, 2026 | CHANGELOG ↗ | RANK

GitGuardian Self-Hosted is a secrets detection platform deployed on-premises that scans code repositories to find and remediate exposed credentials and sensitive data.

> GitGuardian Self-Hosted's 2026.11 release adds 11 new secret detectors and 3 new analyzers, overhauls the Google Artifact Registry integration with keyless auth, and ships several breaking changes — including restricting email/password auth to the dashboard, defaulting Jira/Confluence historical scans to DB-less scanning, and blocking upgrades while background migrations are pending. It also adds a dedicated worker pod for batch tasks and new Helm config options for encryption key isolation and node scheduling.

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

01 Jira Cloud and Confluence Cloud default to DB-less historical scans

Not checked yet — 90

BREAKING

Jira Cloud and Confluence Cloud historical scans now use the DB-less scan framework by default, turning on the DB-less scan flag for each integration in the Admin Area even where it had been turned off. Dedicated pods can be scaled for these scans via Helm, e.g. `celeryWorkers.scanners-db-less-jira-cloud.replicas` and `celeryWorkers.scanners-db-less-confluence-cloud.replicas` in `values.yaml`.

Run Jira Cloud and Confluence Cloud DB-less historical scans on dedicated pods to avoid contending with other scanner workloads.

yaml

```yaml
celeryWorkers:
  scanners-db-less-jira-cloud:
    replicas: 2
  scanners-db-less-confluence-cloud:
    replicas: 2
```

— Names the flag, Admin Area location, and a runnable Helm config snippet.

changelog-20261119-8076961f

02 Dedicated node group scheduling via global Helm values

Not checked yet NEW 85

Global Helm values `global.nodeSelector`, `global.tolerations`, and `global.priorityClassName` can be set to schedule ClickHouse, Keeper, and MinIO pods onto a dedicated node group.

Schedule ClickHouse, Keeper, and MinIO pods onto a dedicated node group by propagating global Helm placement values.

```yaml
global:
  nodeSelector:
    dedicated: gitguardian
  tolerations:
    - key: dedicated
      operator: Equal
      value: gitguardian
      effect: NoSchedule
  priorityClassName: high-priority
```

— Named config keys with a complete runnable snippet. changelog-20261119-8076961f

03 **ClickHouse encryption key isolation** Not checked yet NEW

80

The `miscEncryption.existingSecretKeys.clickhouseEncryptionKeys` key in `values.yaml` isolates ClickHouse encryption from PostgreSQL, so a leaked PostgreSQL key does not expose ClickHouse data.

Isolate ClickHouse encryption from PostgreSQL so a leaked PostgreSQL key does not expose ClickHouse data.

```yaml
miscEncryption:
  existingSecretKeys:
    clickhouseEncryptionKeys: my-clickhouse-key-secret
```

— Named config key with file and a runnable snippet. changelog-20261119-8076961f

04 **Google Artifact Registry integration: keyless auth and health checks**

Not checked yet IMPROVED 70

Google Artifact Registry integrations now support keyless connection with Workload Identity and flag unhealthy installations; admins can update a service account key without reinstalling. The migration to the new integration version must finish before upgrading to 2027.4.

— Explains mechanism and an upgrade caveat, no exact command. changelog-20261119-8076961f

05 **Dedicated worker pod for batch tasks** Not checked yet IMPROVED

65

Batched tasks such as validity checks now run on a dedicated `worker-batch-task-worker` pod (1 replica, autoscales to 5) instead of blocking `worker-celery` pods.

— Names the pod and scaling behaviour, no user-facing action needed.

changelog-20261119-8076961f

06 **Dashboard-only email/password authentication** Not checked yet

60

BREAKING

Email and password authentication is now accepted only to sign in to the dashboard; scripts that called other endpoints with an email and password must switch to using an API token instead.

— Clear before/after and required remediation, no endpoint names.

changelog-20261119-8076961f

07 **Upgrade blocked while background migrations are pending**

Not checked yet

60

BREAKING

An upgrade to 2026.11 is refused while background data migrations started in 2026.8 and 2026.9 are still running; operators must wait for them to finish on the current version before retrying.

— Specific versions named with a clear remedy, no further mechanism.

changelog-20261119-8076961f

THINNER COVERAGE BELOW

08 **New secret detectors and analyzers** Not checked yet NEW

45

Adds 11 new secret detectors across v2.174 and v2.175, including Codex, Composio, and `HubSpot` keys, plus 3 new analyzers: `GoCardless`, Adobe, and Weights & Biases.

— Names several detectors but no mechanism or full list of all 11.

changelog-20261119-8076961f

09 **Public API ticket unlink and clear-text occurrence retrieval**

Not checked yet NEW

30

The public API can now unlink a ticket from an incident and return the content of an occurrence in clear text.

— Describes capability but no endpoint path or method given. changelog-20261119-8076961f

└──▷ ALSO FROM THESE RELEASES

.
.
.

└──▷ BREAKING ON UPGRADE

! Email and password authentication is now accepted only to sign in to the dashboard; scripts that called other endpoints with an email and password must use an API token instead.

! Jira Cloud and Confluence Cloud historical scans now use the DB-less scan framework by default, turning on the `DB-less scan` flag for each integration in the Admin Area even where it had been turned off.

! An upgrade to 2026.11 is refused while background data migrations started in 2026.8 and 2026.9 are still running; wait for them to finish on the current version before retrying.

! The Google Artifact Registry migration to the new integration version must finish before upgrading to 2027.4.

WAS THIS USEFUL? 👍 👎

infisical

Feedback ⓘ v0.167.13 NOTES ↗ RANK

Infisical is the open-source platform for securing secrets, certificates, access, and AI Agents.

> Infisical's latest release adds new secret sync targets for Convex and Cloudflare Workers Preview environments, org-level certificate search, automatic revocation of Intune SCEP certificates, honey-token alert routing, and several Agent Vault visibility and session improvements.

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

01 **Secrets sync for Convex and Cloudflare Workers Preview**

Not checked yet NEW 55

Adds a Convex secret sync integration, letting teams push secrets directly to Convex projects, and extends the existing Cloudflare Workers sync target to also sync secrets to a Preview environment.

— Names two sync targets but no setup steps given v0.167.13

02 **Agent Vault session and admin visibility improvements**

Not checked yet IMPROVED 55

Agent Vault sessions now include named project services and selected skills when a session is created. OAuth variables can now be reused across services. The Organization Overview card shows a skills count, and admins are emailed when free-request usage hits 75% and 100% of the plan limit.

— Groups four thin Agent Vault additions, no config keys named v0.167.13

03 **Automatic revocation of Intune SCEP certificates** Not checked yet

NEW 50

Infisical's PKI now revokes Intune SCEP certificates automatically when Intune queues their revocation.

— Mechanism described but no config or endpoint named v0.167.13

04 **Org-level certificate search with computed status** Not checked yet

NEW 45

Adds org-level certificate search with computed status, letting practitioners find and inspect PKI certificates across the whole organization from one view.

— No UI path or endpoint named v0.167.13

05 **Honey-token alerts routed through alerts system** Not checked yet

IMPROVED 30

Honey-token trigger notifications are now routed through the alerts system instead of being sent directly.

— Thin one-line change, no mechanism or config detail v0.167.13

WAS THIS USEFUL? 👍 👎

◆ Code Security

StackHawk

Feedback ⓘ changelog · Nov 19, 2026 CHANGELOG ↗

StackHawk is an application security tool built for developers. Automated scanning for the entire dev pipeline combined with continuous documentation and remediation.

StackHawk adds per-rule alert limits, MCP type-array support, new `HAWK_INSTALL_CHANNEL` and `HAWK_NO_MODIFY_PATH` env vars, and several `hawk op` CLI improvements.

Control how many alerts each scan rule reports to the platform by setting per-rule alert limits from the StackHawk scan policy — HawkScan keeps testing after the limit and surfaces the highest risk and confidence alerts first. Not checked yet

Set `HAWK_INSTALL_CHANNEL=dev` to install the newest development build of HawkScan instead of the newest stable release. Not checked yet

Set `HAWK_NO_MODIFY_PATH=1` to prevent install scripts from adding the install directory to your shell profile or Windows user Path. Not checked yet

Install scripts now place HawkScan in `~/.local/bin` (or `%USERPROFILE%\.local\bin` on Windows) by default instead of the previous location. Not checked yet

MCP server scanning now accepts JSON Schema `type` arrays (e.g. `["string", "null"]`) used by the MCP C# SDK for optional parameters, so discovery no longer halts on those schemas. Not checked yet

+6 more

UPDATED VULNERABILITY CHECK Passive rules now read Brotli-compressed response bodies on ARM64

└──▷ **BREAKING ON UPGRADE**

! Install scripts now install HawkScan to `~/.local/bin` by default; pipelines that added the previous location to PATH (e.g. via `$GITHUB_PATH` or `$BASH_ENV`) must be updated to use `~/.local/bin` instead.

! `hawk op repo link --app-name` no longer creates a new application if the name is not found — it fails and changes nothing; run `hawk op app create` first to create the application.

WAS THIS USEFUL? 👍 👎

Semgrep

Feedback ⓘ updated · Nov 19, 2026 NOTES ↗ RANK

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

> Semgrep adds structured JSON scan logging via `SEMGREP_LOG_JSON_FILE`, lets any MCP client run jobs with `semgrep_run_job`, and expands Supply Chain to flag Python dependencies declared with version ranges or no pinned version; smaller updates cover PHP trait cross-file analysis, Go parsing, Editor filtering, and Policies page visibility.

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

01 **Structured JSON scan logging via env variable** Not checked yet

NEW 90

Setting the `SEMGREP_LOG_JSON_FILE` environment variable to a file path makes Semgrep write one JSON object per line for each scan phase start, finish, warning, and error, tagged with scan details, for use with tools like `jq` or log pipelines.

— Names exact env var and line-delimited JSON output format snapshot-20261119

02 **Version-range dependency findings in Supply Chain** Not checked yet

NEW 85

Semgrep Supply Chain now reports findings for Python dependencies declared in `requirements.txt` with a version range (e.g. `litellm>=1.10`) or without a version (e.g. `flask`), labeled Needs review; requires Semgrep CLI version 1.184.0 or later.

— Names file, concrete examples, and minimum CLI version snapshot-20261119

03 **Run scan and workflow jobs via MCP tool** Not checked yet NEW

70

Any MCP client can now run scan and workflow jobs using the `semgrep_run_job` tool, including clients that do not support MCP tasks.

— Named tool but no further usage detail given snapshot-20261119

04 **SSRF-scoped memories for AI detection triage** Not checked yet

NEW 65

Users can write memories scoped to server-side request forgery (SSRF) triage by selecting SSRF under AI Detection in Rules when adding a memory in Rules & Policies > Memories.

— Exact UI navigation path given, limited mechanism detail snapshot-20261119

05 **Paginated rule browsing and filtering in Editor** Not checked yet

IMPROVED

65

The Semgrep Editor now loads rules in pages and supports filtering by language, source, severity, visibility, and authorship, as well as grouping by folder or ruleset.

— Lists specific filter and grouping options, UI-only snapshot-20261119

06 **Guardian-only rules visible in Policies page** Not checked yet

NEW

65

Guardian-only Semgrep Code rules are now visible in the Policies page rules list, labeled Guardian only, and can be added to the Semgrep Code policy by enabling CI on them.

— Exact UI label and enablement path given snapshot-20261119

THINNER COVERAGE BELOW

07 **Audit logging for hosted MCP server actions** Not checked yet

IMPROVED

55

Audit logs now record when an action was taken through the hosted MCP server, naming the MCP tool and client that took the action; MCP tool calls that change data now write an audit event even when the underlying action did not previously do so.

— Describes behavior change but no UI path or endpoint snapshot-20261119

08 **Go parsing support for generics and chained indexing**

Not checked yet IMPROVED

55

Go parsing now supports generic type aliases, mixed unnamed map parameters or results, and chained indexing such as `table[key][next]` represented as nested index expressions.

— Names specific language constructs, no usage example snapshot-20261119

09 **Specific error messages for Supply Chain scan failures**

Not checked yet IMPROVED

50

Supply Chain scan error alerts on the Projects page now show a message per error type (e.g. Lockfile parsing failed or Dependency resolution failed) instead of a generic warning.

— Concrete example messages but no resolution guidance snapshot-20261119

10 **Cross-file analysis for PHP trait methods** Not checked yet

IMPROVED

40

Semgrep Code now follows calls to PHP methods that come from traits, expanding cross-file analysis coverage to trait-based code.

— States capability only, no example or scope detail snapshot-20261119

WAS THIS USEFUL?  

GitHub Feedback ⓘ

Wait for pull request events with GitHub CLI (2026-11-19) BLOG ↗ RANK

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

> GitHub shipped an event-driven alternative to PR polling in the CLI, added the Gemini 4 Neon model to Copilot, turned on automatic security risk assessments for GitHub Team orgs, and let teams set shared Copilot Agent Plugin defaults.

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

01 Event-driven PR waiting in GitHub CLI Not checked yet NEW

93

`gh event listen <PR-URL> --count <n> --follow --timeout <duration> --jq <expr> --template <tmpl>` waits for pull request events via Event Streams instead of polling in a loop, printing each event as a line of JSON and exiting after the first by default. Subscriptions can be managed directly with `gh event subscription create`, `list`, `view`, and `delete`. Supported event types include submitted reviews, pull request state and head changes, merge conflicts, and completed check suites, and `gh pr create`, `gh pr view`, `gh run view`, `gh run watch`, and `gh api` now suggest `gh event listen` instead of polling when an event-driven alternative exists.

Block a CI script until a PR review is submitted, then act on the reviewer's decision without a polling loop.

```
$ gh event listen https://github.com/owner/repo/pull/42 --jq
'.action' --timeout 30m
```

Keep a long-running agent session open to process multiple PR events — such as successive check-suite completions — in sequence.

```
$ gh event listen https://github.com/owner/repo/pull/42 --count 5
--follow --jq '{event: .action, sha: .pull_request.head.sha}'
```

Inspect and clean up active Event Streams subscriptions after an automated workflow finishes.

```
$ gh event subscription list
gh event subscription delete <subscription-id>
```

— Full command, flags and subcommands with runnable examples

Wait for pull request events with GitHu…

02 **Team-level Agent Plugin defaults for Copilot** Not checked yet

NEW 72

Maintainers can set shared Agent Plugin defaults for a team by opening the team page on github.com and selecting the Customize Copilot tab; plugins are enabled by default for direct members in VS Code, the GitHub Copilot app, and Copilot CLI. A plugin marketplace can be added from any GitHub repository containing a plugin marketplace via the same tab, making its plugins available to browse and enable for the team. Team plugin defaults are optional and member-overridable where policy permits, and enterprise and organization policies still take precedence over team choices.

When onboarding a new team, set shared Agent Plugin defaults once so every direct member gets the right plugins in VS Code and Copilot CLI without individual setup.

📍 1. Go to your organization on github.com and open the target team. 2. Select the Customize Copilot tab. 3. Browse plugins from your enterprise or team marketplaces and add the plugins your team requires. 4. Optionally, add a marketplace by supplying a GitHub repository that contains a plugin marketplace.

— Exact UI path and precedence rules given, no API/flag

Customize GitHub Copilot for your team …

THINNER COVERAGE BELOW

03 **Gemini 4 Neon model in Copilot** Not checked yet NEW 53

GitHub Copilot adds Gemini 4 Neon, a model built for agentic coding, multistep tool use, and knowledge work. It can be selected from the model picker in Visual Studio Code, JetBrains, Xcode, Eclipse, Copilot CLI, github.com, GitHub Mobile, or the Copilot app, offering faster first-token response and fewer unrequested code changes.

Select Gemini 4 Neon for an agentic coding task in Copilot CLI to get faster first-token response and fewer unrequested code changes.

> 📍 In the model picker (Visual Studio Code, JetBrains, Xcode, Eclipse, Copilot CLI, github.com, GitHub Mobile, or the Copilot app), select `Gemini 4 Neon` from the list of available models.

— Names surfaces and benefit but no mechanism detail

Gemini 4 Neon in GitHub Copilot (2026-1…

04 **Automatic security risk assessments on GitHub Team**

Not checked yet NEW 30

Security risk assessments now run automatically for organizations on GitHub Team, letting organization admins and security managers review findings on exposed credentials and code vulnerabilities without manual setup.

— Describes what it does but no config or navigation detail

Security risk assessments run automatic…

NEW INTEGRATION Box MCP connector

NEW INTEGRATION Buildkite MCP connector

NEW INTEGRATION Calendly MCP connector

NEW INTEGRATION ClickUp MCP connector

NEW INTEGRATION Mixpanel MCP connector

NEW INTEGRATION Supabase MCP connector

NEW INTEGRATION Webflow MCP connector

NEW INTEGRATION Wix MCP connector

> Connect Supabase, Box, Calendly, and more to Copilot (2026-11-18) BLOG ↗
>
> STABLE
>
> GitHub Copilot adds eight GitHub-verified MCP server connectors in public preview, reachable from the Copilot app, CLI (`/mcp`), VS Code Agents window, and github.com.
>
> Add new MCP connectors to Copilot from the CLI by running `/mcp` , switching to the

> Connectors tab, and selecting Connect on the service you want. Not checked yet
>
> Add new MCP connectors in VS Code by opening the Agents window, going to Customizations, and connecting the service you want. Not checked yet

---

WAS THIS USEFUL? 👍 👎

opentaint

Feedback ⓘ analyzer/2026.11.18.f5b1e13 NOTES ↗ RANK

Opentaint is the open source taint analysis engine for the AI era. A formal dataflow analysis tool you can customize and self-host, built so AI agents drive your application security analysis without burning tokens on every scan.

> Opentaint added toolchain provenance tracking for Go projects, recording the Go toolchain version in its project model.

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

01 **Go toolchain version in project model** Not checked yet NEW

30

Opentaint now records the Go toolchain version in the project model, making toolchain provenance visible alongside scan results.

— Describes what changed but no mechanism or UI path given analyzer/2026.11.18.f5b1e13

NEW SUPPORTED PLATFORM Go built-in taint models

autobuilder/2026.11.18.f5b1e13 NOTES ↗ STABLE

opentaint adds a `--semgrep-rule-id-exclude` flag, deep exclusions for taint rules, and a `$*` star operator for field matching.

└──▷ **GET THIS VERSION** ▾

```
$ git clone --branch autobuilder/2026.11.18.f5b1e13
https://github.com/seqra/opentaint.git
# already have the repo? check out this version:
$ git checkout autobuilder/2026.11.18.f5b1e13
```

Exclude specific Semgrep rules from analyzer-side taint analysis with the `--semgrep-rule-id-exclude` flag. Not checked yet

Implement deep field exclusions in taint rules so nested field paths can be suppressed from propagation. Not checked yet

Use the new `$*` star operator in taint rules to match any field on an object. Not checked yet

WAS THIS USEFUL? 👍 👎

qodana-cli

Feedback ⓘ v2026.2.4 NOTES ↗ RANK

Qodana-cli jetbrains Qodana's official command line tool

> Qodana-cli v2026.2.4 adds the ESLint plugin to its included plugin list, enabling ESLint-based linting rules in JavaScript/TypeScript scans.

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

01 **ESLint plugin added for JS/TS scans** Not checked yet NEW

40

The ESLint plugin is now included in Qodana's plugin lists, enabling ESLint-based linting rules during Qodana JavaScript/TypeScript scans.

— Names the plugin and scan types but no config detail v2026.2.4

WAS THIS USEFUL? 👍 👎

GitLab Feedback ⓘ

The recommended GitLab configuration for agentic engineering (2026-11-18)

BLOG ↗ RANK

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

> GitLab published a recommended agentic engineering configuration that wires local coding harnesses like Claude Code into Duo Agent Platform via installable skills, an MCP server connection, automatic code review, and assignable agent flows for MR and pipeline work.

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

01 gitlab-duo-setup skill for group-wide Duo config Not checked yet

NEW 90

Install the `gitlab-duo-setup` slash-command skill in Claude Code (or any compatible harness) by cloning `https://gitlab.com/gitlab-da/projects/agentic-eng-config.git` and copying it to `~/.claude/skills/`; running `/gitlab-duo-setup` presents a step-by-step plan to automate group-wide Duo Agent Platform configuration in one step.

Bootstrap a GitLab group for agentic workflows from your terminal — the skill clones the config repo, copies skills, and then automates group-wide Duo Agent Platform setup in one approved plan.

```
$ git clone https://gitlab.com/gitlab-da/projects/agentic-eng-config.git
cp -R agentic-eng-config/skills/gitlab-duo-setup ~/.claude/skills/
cp -R agentic-eng-config/skills/gitlab-mr-followup ~/.claude/skills/
# then, inside Claude Code in your project directory:
/gitlab-duo-setup
```

— Exact clone/copy commands and slash command name given

The recommended GitLab configuration fo…

02 Automatic Duo code review on merge requests Not checked yet NEW

88

Enable automatic code review per project at Settings > Merge requests > GitLab Duo Code Review > `Enable automatic reviews by GitLab Duo`, with an optional `Start a new review on push` setting to trigger a follow-up review on every commit to the MR branch.

Enable automatic Duo code review and per-push re-review for a single project, so every commit to an MR branch gets a follow-up review that builds on the earlier one.

> 📍 1. Go to your project in GitLab. 2. Navigate to Settings › Merge requests › GitLab Duo Code Review. 3. Enable `Enable automatic reviews by GitLab Duo`. 4. Enable `Start a new review on push`.

– Exact settings path and toggle names with step-by-step example

The recommended GitLab configuration fo…

---

03 **GitLab MCP server connection for coding harnesses** Not checked yet

NEW

83

Connect a local coding harness to GitLab via the GitLab MCP server, giving Claude Code (or another harness) access to issue and MR context, work-item tools, and the `Start Duo session` tool over a single OAuth connection. Unlock the connection for a group by enabling `Allow connection to GitLab` under the group's Settings > General > Permissions and group features (required when a 403 appears at sign-in).

– Names OAuth connection, specific tools, and exact settings path

The recommended GitLab configuration fo…

---

04 **Agent flows for MR, pipeline, and security triage** Not checked yet

NEW

83

Enable agents to open merge requests, resolve conflicts, repair failed pipelines, and triage security findings (Ultimate only) by assigning the `Developer flow`, `Code Review flow`, or `Fix CI/CD Pipeline` flow through the Duo Agent Platform.

– Names three specific flows and their tier scope

The recommended GitLab configuration fo…

---

05 **Per-repo code review config files** Not checked yet NEW

80

Configure per-repo code-review behaviour with `mr-review-instructions.yaml` (focus areas, per-path rules, standards) and `.gitlab/duo/mr-review-automated-rules.yaml` (exclude MRs by target branch, source branch, or author).

– Named config files and fields but no worked example

The recommended GitLab configuration fo…

06 **MR followup skill for local agent monitoring** Not checked yet

NEW

70

Copy `agentic-eng-config/skills/gitlab-mr-followup` to `~/.claude/skills/` to install the MR followup skill, which lets a local agent monitor merge-request progress and act on findings without leaving the harness.

Bootstrap a GitLab group for agentic workflows from your terminal — the skill clones the config repo, copies skills, and then automates group-wide Duo Agent Platform setup in one approved plan.

```
$ git clone https://gitlab.com/gitlab-da/projects/agentic-eng-
config.git
cp -R agentic-eng-config/skills/gitlab-duo-setup
~/.claude/skills/
cp -R agentic-eng-config/skills/gitlab-mr-followup
~/.claude/skills/
# then, inside Claude Code in your project directory:
/gitlab-duo-setup
```

— Install path given but how it 'acts on findings' is unspecified

The recommended GitLab configuration fo…

WAS THIS USEFUL?  

Veracode

Feedback ⓘ Veracode SAST (2026-11-18) BLOG ↗ RANK

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

> Veracode's biggest moves this window were a new Package Firewall that blocks untrusted packages across repositories, a batch of new Veracode CLI commands and packaging flags, and expanded SAST language coverage including C# and Spring AI; DAST, IDE, SCM/CI, EASM, and eLearning all also received incremental but concrete additions.

└──▷ **WHAT SHIPPED · 30 FEATURES** most completely described first ? what's the number?

01 veracode package new flags and options

Not checked yet NEW

85

Package C# source code directly for Static Analysis without compiling into binaries using the new `--csharp-source` flag on `veracode package`; exclude specific Java packages or JAR files with the new `--exclude` flag; exclude artifacts such as unsupported SQL from packaging results without affecting other languages using the new `--skip-packagers` flag; add support for `requirements-dev.txt` in Python packaging workflows to include development dependencies; and set `VERACODE_PACKAGE_GOLANG_GENERATE=true` to enable CGO code generation when packaging a Go project that uses cgo so native libraries are captured in the scannable artifact.

Enable CGO code generation when packaging a Go project that uses cgo so native libraries are captured in the scannable artifact.

```
$ VERACODE_PACKAGE_GOLANG_GENERATE=true veracode package --source
<path/to/go/project> --output <output-dir>
```

— Names every flag and env var with exact syntax Veracode CLI (2026-11-05)

02 New veracode.yml configuration keys for CI workflows

Not checked yet NEW

85

Adds `policy` to apply an infrastructure-as-code scan policy in GitHub, GitLab, and Azure DevOps workflows; `predependency_command` to run setup commands before packaging in GitHub and GitLab workflows; a custom agent pool name parameter to target a build agent pool in Azure DevOps; `build_runs_on` to target a specific build runner for SCA scans in GitHub workflows; `debug` to enable debugging output in GitHub, GitLab, and Azure DevOps workflows; and `analysis_branch` to run scheduled Azure DevOps scans against a specific branch.

Enforce an IaC scan policy in a GitLab or GitHub workflow so the pipeline fails when findings violate your Veracode policy.

```yaml
# veracode.yml
iac:
  policy: '<your-policy-name>'
```

Run a dependency installation command before Veracode packages the project — useful when the build requires a setup step not handled automatically.

```yaml
# veracode.yml
predependency_command: 'npm install --legacy-peer-deps'
```

Turn on debug output in a workflow run to diagnose packaging or scan failures without changing any other settings.

```yaml
# veracode.yml
debug: true
```

— Six named config keys with runnable YAML examples SCM and ticketing (2026-11-03)

---

03 **veracode fix sca command (Limited Availability)** Not checked yet

NEW 70

New `veracode fix sca` command generates fixes for vulnerable dependencies identified in SCA scans; running it with `--fire-and-forget` submits remediation requests in the background so a CI job returns immediately rather than waiting for fixes and pull requests to be created.

Submit SCA remediation requests in the background so a CI job returns immediately rather than waiting for fixes and pull requests to be created.

```
$ veracode fix sca --fire-and-forget
```

— Named command, flag, and runnable example Veracode CLI (2026-11-05)

---

04 **veracode.json exclusions for Java jars and classes**

Not checked yet NEW 60

Exclude specific Java `.jar` files and specific Java classes from static analysis by listing them in `veracode.json`.

— Named config file with exact use, no sample syntax Veracode SAST (2026-11-18)

05 **EASM platform enhancements** Not checked yet NEW 60

EASM adds component risk scoring against the EASM vulnerability knowledge base reflecting real vulnerabilities per version rather than age alone; compliance evidence collection covering cookie consent tracking, third-party data flows, destination countries, and privacy, legal, and copyright documentation to support GDPR, NIS2, and DORA assessments; export of web applications from EASM into DAST Essentials by marking assets as DAST Candidates to create discovered scan targets; and real-time in-app notifications when scans complete, fail, or are cancelled.

— Explains scoring logic and before/after, no UI path Names evidence categories and frameworks covered Names the action but no exact UI location Bare description of notification states only

Veracode EASM (2026-10-26)

THINNER COVERAGE BELOW

06 **Static scan findings filtering and mitigation view in VS Code**

Not checked yet NEW 55

Filter Static Scan Findings in VS Code to the Current File open in the editor, filter and group findings by file name with each file's findings grouped by severity, and see a new Mitigated Findings section in the Flaws That Violate Policy view for findings with approved mitigations.

— Describes UI behaviour but no exact path steps IDEs (2026-11-05)

07 **OAuth authentication region switching and SSO in IDEs**

Not checked yet NEW SUPPORTED PLATFORM NEW 55

Change the OAuth authentication region in VS Code and see the current or most recently used region on the OAuth authentication screen below Authentication ; Veracode Scan now supports OAuth-based authentication with Single Sign-On (SSO) for Visual Studio, VS Code, Eclipse, and JetBrains.

— Names IDEs and auth mechanism but no exact steps IDEs (2026-11-05)

08 **Environment setup checks in VS Code** Not checked yet NEW 55

Run environment setup checks in VS Code to identify connectivity, proxy, DNS, firewall, and TLS issues when connecting to Veracode services.

— Names specific checks but not how to invoke them IDEs (2026-11-05)

09 **New veracode CLI commands** Not checked yet NEW 55

Adds `veracode scan static` to run static scans and review findings within a Git workflow, `veracode findings static` to access cached static scan findings in the local Veracode directory, and `veracode package discover` to detect the toolchains required to create scannable artifacts.

— Named runnable command, no usage example given Named runnable command, lacks example invocation Named runnable command, no example shown

Veracode CLI (2026-11-05)

---

10 **Enhanced Python scanner with improved taint tracking**

Not checked yet IMPROVED 55

Enhanced Python scanner adds support for PySpark, Flask, Django, and FastAPI applications with improved taint tracking, cross-file analysis, and pattern recognition.

— Names mechanism improvements, no usage steps Veracode SAST (2026-11-18)

---

11 **SCA Skip Vulnerable Method Analysis setting** Not checked yet NEW

50

New setting to skip vulnerable method analysis during SCA scans in Visual Studio (SCA Skip Vulnerable Method Analysis), `JetBrains` IDEs, and Eclipse to reduce scan time.

.

— Named setting per IDE but no exact path IDEs (2026-11-05)

---

12 **Import static scan results into IDEs with mitigation proposals**

Not checked yet NEW 50

Import static scan results from the Veracode Platform directly into Visual Studio, JetBrains IDEs, and VS Code, and propose mitigations for static scan flaws within the IDE.

.

— Clear capability, lacks exact command or menu path IDEs (2026-11-05)

---

13 **Package Firewall launch with proactive Maven monitoring**

Not checked yet NEW 50

Veracode Package Firewall is now available, automatically blocking untrusted packages that violate policies across artifact repositories and package managers to mitigate malware, typosquatting, and license violations. Package Firewall, SCA, and SSCI now also proactively monitor Maven packages, ingesting new versions regularly for malware analysis.

— Describes mechanism and scope, no config surface Veracode Package Firewall (2026-11-06)

---

14 **Broadened language and framework support in SAST** Not checked yet

NEW 50

Veracode SAST adds support for Angular 21, NestJS 11.1.x, Node.js 24.x, Scala 3.10, C# source code scanning in .NET projects, JDK 27, LLM-powered applications built with Spring AI, iOS 27, Go 1.27, Dart 3.13 and Flutter 3.47, and the Python `google-cloud-bigquery` library.

— Many named versions, but just coverage additions Veracode SAST (2026-11-18)

15 **33 deprecated eLearning courses removed** Not checked yet

DEPRECATED

50

33 deprecated courses are no longer available, including OWASP 2017, OWASP Top 10 (2021) (6 courses), Secure Coding for .NET (6 courses), Secure Coding for Java (6 courses), Secure Coding for JavaScript (5 courses), Secure Coding for PHP (6 courses), and Secure Coding for Python (3 courses).

— Enumerates exact counts per course category Veracode eLearning (2026-11-18)

16 **Scan Scope setting in Visual Studio** Not checked yet NEW

45

New Scan Scope setting in Visual Studio lets you scan the full project directory or only the active solution for faster, more focused results.

— Named setting, no exact location given IDEs (2026-11-05)

17 **RBAC for container and IaC scans in CLI** Not checked yet

NEW SUPPORTED PLATFORM NEW

45

Add RBAC support to `veracode scan` for container and IaC scans so developers can access only the application profiles associated with their teams.

— Names command and scope, no config detail Veracode CLI (2026-11-05)

18 **Target UUIDs for veracode dynamic scan** Not checked yet IMPROVED

45

Support target UUIDs alongside webhook UUIDs when triggering scans with `veracode dynamic scan`.

— Named command and identifier type, no example Veracode CLI (2026-11-05)

19 **OWASP Top 10:2025 secure coding courses** Not checked yet

UPDATED COMPLIANCE FRAMEWORK NEW

45

New secure coding courses aligned to OWASP Top 10:2025 are now available for .NET, Java, JavaScript, PHP, and Python, replacing the deprecated 2021-list courses.

— Names languages covered, no course list or path Veracode eLearning (2026-11-18)

20 **Schedule scans from Veracode Platform via veracode.yml**

Not checked yet NEW

45

Schedule scans for installed organizations directly from the Veracode Platform based on `veracode.yml` configuration, including Azure DevOps Workflow Integration scans and Static Analysis, SCA, and IaC scans for GitHub organizations.

– Names scan types covered, no exact UI steps SCM and ticketing (2026-11-03)

21 **GitHub Workflow Integration management** Not checked yet NEW

45

The Veracode GitHub Workflow Integration can now be installed, configured, updated, and uninstalled directly from the Veracode Platform without going through the GitHub Marketplace, using a new uninstallation workflow, and now autopackages Apex, VB6, and Perl projects.

– Describes lifecycle actions, no exact navigation Names languages only, no mechanism detail

SCM and ticketing (2026-11-03)

22 **DryRun Security integration for AI-native PR workflows**

Not checked yet NEW

40

New DryRun Security integration surfaces Veracode Static Analysis findings and remediation guidance inside AI-native pull request and code review workflows.

– Names integration and surface area, thin on mechanism Veracode SAST (2026-11-18)

23 **Expanded hardcoded secrets detection** Not checked yet IMPROVED

40

Hardcoded secrets detection now includes application configuration files with `-local` and `-prod` naming patterns.

– Names patterns detected, no further scope given Veracode SAST (2026-11-18)

24 **Pipeline Scan supports larger artifacts** Not checked yet IMPROVED

40

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

– Gives concrete size limit but no further mechanism Veracode SAST (2026-11-18)

25 **Captions in six languages for eLearning courses** Not checked yet

IMPROVED

40

Nine eLearning courses — including Software Security Awareness - OWASP Top 10:2025, Threat Modeling, and C/C++ Memory Management Risks and Best Practices — now have captions in English, French, German, Japanese, Portuguese, and Spanish.

– Names courses and languages, no further scope Veracode eLearning (2026-11-18)

26 **IDE version support matrix** Not checked yet IMPROVED

35

Veracode Scan now supports IDE versions 2024.2 through 2026.3 for JetBrains, and Visual Studio 2026 for Visual Studio.

— Version ranges named but no behaviour change explained IDEs (2026-11-05)

27 **SSCI on unified Veracode REST API** Not checked yet IMPROVED

35

Software Supply Chain Intelligence (SSCI) now runs on the unified Veracode REST API — see the Software Supply Chain Intelligence REST API docs for endpoint details.

— Points to docs but no endpoint named here Veracode Package Firewall (2026-11-06)

28 **One-year report date range in eLearning** Not checked yet IMPROVED

35

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

— Exact limit given, clear starting action Veracode eLearning (2026-11-18)

29 **Jira Server integration supports Jira 11** Not checked yet IMPROVED

30

Veracode Integration for Jira Server v5.0.2 now supports Jira 11, including the required Java 21 compatibility.

— Named version compatibility, no setup detail SCM and ticketing (2026-11-03)

30 **eLearning REST API end of support** Not checked yet DEPRECATED

25

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

— States EOL with no migration guidance given Veracode eLearning (2026-11-18)

NEW COMPLIANCE FRAMEWORK Six new built-in security policies

NEW SUPPORTED PLATFORM Reporting REST API now available in the European Region

NEW VULNERABILITY CHECK COBOL CWE detections

└──▷ BREAKING ON UPGRADE

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

! 33 deprecated courses are no longer available, including OWASP 2017, OWASP Top 10 (2021) (6 courses), Secure Coding for .NET (6 courses), Secure Coding for Java (6 courses), Secure Coding for JavaScript (5 courses), Secure Coding for PHP (6 courses), and Secure Coding for Python (3 courses).

! The DAST REST API scheduling endpoints have changed as of June 24, 2026; integrations that manage schedules via the REST API must be updated to use the new endpoints.

Veracode Platform (2026-11-09) BLOG ↗ STABLE

Veracode adds v2 Reporting API endpoints, a Custom PDF REST API, OAuth support for XML APIs, new report filters and fields, MPT Flaw Matching, and container/IaC results on the platform.

New v2 Reporting API adds dedicated endpoints for findings, scans, deleted scans, and audit log reports, replacing the deprecated `POST /appsec/v1/analytics/report`. Not checked yet

The v2 findings endpoint `POST /analytics/findings/report` now accepts optional date filters `first_found_start_date`, `first_found_end_date`, `resolved_start_date`, and `resolved_end_date` to narrow results within the required `last_updated_start_date` / `last_updated_end_date` range. Not checked yet

New `most_recent_scan` filter available on the Reporting API Scans report — set to `true` to return only the most recent scan per asset, reducing client-side filtering. Not checked yet

New `custom_severity` filter available on the Reporting API Findings report. Not checked yet

New `collections_list` field added to the Finding Reporting API response, returning a list of collection names associated with an application. Not checked yet

+15 more

└─▷ **BREAKING ON UPGRADE**

! The `/healthcheck/status` endpoint has been removed and now returns a 404 error; use the `v2/principal` endpoint in the Identity REST API to check authenticated connectivity instead.

! `report_type` is no longer accepted in the request body for the v2 Reporting API endpoints (it was accepted in v1).

Veracode Fix (2026-10-22) BLOG ↗ STABLE

Veracode Fix adds a `veracode fix sca` CLI command for SCA remediation and now processes GitHub Workflow Integration fix requests asynchronously.

Run SCA remediation from the CLI with the new `veracode fix sca` command, which analyzes vulnerable dependencies, generates patches, and identifies safe upgrade paths. Not checked yet

Veracode Fix for SCA now processes GitHub Workflow Integration fix requests asynchronously, freeing the GitHub Actions runner immediately and delivering fixes as a new pull request with a results comment on the original. Not checked yet

WAS THIS USEFUL?

◆ WAF, Bot & API Protection

DataDome

Feedback ⓘ Go module 2.6.0 (2026-11-19) BLOG ↗ RANK

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

> DataDome raised the header-forwarding limit across three edge modules and added a way to skip WAF inspection on out-of-band Fastly requests.

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

01 WAF inspection bypass flag for Fastly Protection API

Not checked yet NEW 65

The Fastly module adds `waf.inspection.disabled`, which can be sent on requests to the Protection API to skip Next-Gen WAF inspection on out-of-band architecture requests.

— Names exact flag and target API but no further detail Fastly module 3.2.1 (2026-11-18)

THINNER COVERAGE BELOW

02 HeadersList truncation limit raised across modules

Not checked yet IMPROVED 55

The `HeadersList` truncation limit was increased from 512 to 768 bytes in the Go module, the Cloudflare Worker Rust module, and the Envoy module, allowing more header data to be forwarded for bot-detection analysis without being cut off.

— Names exact config field and byte limits, no mechanism beyond that

Go module 2.6.0 (2026-11-19) Cloudflare Worker Rust module 1.1.0 (20… Envoy module 2.9.0 (2026-11-19)

WAS THIS USEFUL?

Fastly

Feedback ⓘ Fastly Terraform Provider (beta) 0.2.10 (2026-11-18)

BLOG ↗ RANK

Fastly is a cloud edge computing platform that provides CDN, DDoS protection, load balancing, and real-time content delivery for websites and applications.

> Fastly's Terraform Provider BETA 0.2.10 adds account-level product enablement resources, a new Object Storage logging destination, per-service alert scoping, and migration tooling for moving legacy Compute and VCL services onto CDN Auto and Compute Auto.

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

01 Object Storage logging destination for Compute services

Not checked yet NEW 75

A new `logging_fos` block routes Compute service logs to Fastly Object Storage instead of a third-party sink, configured with `bucket` and `path` fields on `fastly_service_compute_auto`.

Route Compute service logs to Fastly Object Storage instead of a third-party sink.

hcl

```hcl
resource "fastly_service_compute_auto" "example" {
  name = "my-compute-service"

  logging_fos {
    name       = "fos-logs"
    bucket     = "my-log-bucket"
    path       = "/logs/"
  }
}
```

— Names exact block, fields, and resource with runnable config.

Fastly Terraform Provider (beta) 0.2.10…

02 Account-level product enablement resources

Not checked yet NEW 72

Four new resources let you enable account-level products directly in Terraform: `fastly_product_ai_accelerator`, `fastly_product_ai_runtime_control`, `fastly_product_domain_research`, and `fastly_product_object_storage`.

Enable the AI Accelerator product at the account level so all eligible services can use it.

```hcl
resource "fastly_product_ai_accelerator" "enabled" {}
```

— Names all four resources with a runnable example, but no behaviour per product.

Fastly Terraform Provider (beta) 0.2.10…

03 **Per-service alert dimensions** Not checked yet NEW 72

Stats alerts can now be scoped to a set of services individually rather than in aggregate by adding `dimensions.services` to a `fastly_alert` resource.

Alert on stats for a specific set of services individually rather than in aggregate.

```hcl
resource "fastly_alert" "per_service" {
  name        = "high-error-rate"
  metric      = "status_5xx"
  threshold   = 500

  dimensions {
    services = ["abc123", "def456"]
  }
}
```

— Names the field and resource with a runnable example.

Fastly Terraform Provider (beta) 0.2.10…

THINNER COVERAGE BELOW

04 **VCL-to-CDN Auto migration resource splitting** Not checked yet NEW 59

VCL-to-CDN Auto migration now splits legacy Bot Management, DDoS Protection, and Next-Gen WAF product enablement into standalone resources with service-ID imports, and generates standalone CDN simple-product resources with service-ID imports from legacy product enablement.

— Names migration targets but no concrete resource names or example.

Fastly Terraform Provider (beta) 0.2.10…

05 **Compute Auto state migration support** Not checked yet IMPROVED 55

New `moved` block state migration support lets you migrate legacy `fastly_service_compute` state to `fastly_service_compute_auto` without recreating resources.

— Names both resource types and the mechanism but gives no example.

Fastly Terraform Provider (beta) 0.2.10…

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

OWASP dependency-track

Feedback ⓘ 5.2.2 NOTES ↗

RANK

Dependency-Track is an intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.

> Dependency-Track 5.2.2 ships two performance improvements: smarter NVD feed mirroring and faster collection project metrics calculation.

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

01 **Skips redundant yearly NVD feed downloads** Not checked yet

IMPROVED 30

Dependency-Track now skips the yearly NVD feed download when the modified feed already covers the time since the last mirror, reducing unnecessary data transfer.

— Explains behaviour change but no config or metric given 5.2.2

02 **Partition pruning for collection project metrics** Not checked yet

IMPROVED 30

Dependency-Track now uses partition pruning when calculating current collection project metrics, improving query performance.

— Names mechanism but no measured gain or scope 5.2.2

NEW SUPPORTED PLATFORM Red Hat distro-aware version matching

4.14.7 NOTES ↗ STABLE

└──▷ **GET THIS VERSION** ▾

```
$ git clone --branch 4.14.7
https://github.com/DependencyTrack/dependency-track.git
# already have the repo? check out this version:
$ git checkout 4.14.7
```

WAS THIS USEFUL? 👍 👎

LavaMoat

Feedback ⓘ `@lavamoat/react-native-lockdown@3.0.0` NOTES ↗

RANK

LavaMoat is a security tool that protects JavaScript applications by isolating dependencies using object capability principles to prevent supply chain attacks.

> LavaMoat shipped a new CI safeguard and stricter defaults for allow-scripts, plus a parser upgrade for react-native-lockdown that carries a Hermes compatibility warning.

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

01 CI check command and exact-version pinning in allow-scripts

Not checked yet

BREAKING

91

`@lavamoat/allow-scripts@5.1.1` adds a `check` command, runnable as `npx @lavamoat/allow-scripts check`, that warns in CI when the allow-scripts configuration needs updating, catching stale allow-lists before they silently permit or block install scripts. Install scripts are now pinned to exact versions by default, so a dependency upgrade that swaps in a new install script is blocked until the allow-list is explicitly updated. This is a breaking change: allow-scripts no longer matches a lower pinned version against a newer one, existing configurations require a migration action to keep working under default pinning, and Node.js v18 is no longer supported.

Run in CI to detect when an install script has changed version and the allow-list is out of date, failing the pipeline before a stale config silently applies.

```
$ npx @lavamoat/allow-scripts check
```

— Names the exact command and all breaking behavior changes.

`@lavamoat/allow-scripts@5.1.1`

THINNER COVERAGE BELOW

02 @endo/parser-pipeline for Node.js parsing in react-native-lockdown

Not checked yet

BREAKING

52

`@lavamoat/react-native-lockdown@3.0.0` switches Node.js parsing to use `@endo/parser-pipeline`. The release also bundles a SES upgrade that may introduce regressions in Hermes, which is why it's versioned as a major release out of caution — teams should test Hermes-based React Native builds before upgrading.

— Names the new parser package but gives no usage example or command.

`@lavamoat/react-native-lockdown@3.0.0`

└─▷ BREAKING ON UPGRADE

! The SES upgrade may introduce regressions in Hermes; this release is versioned as major (3.0.0) out of caution — test Hermes-based React Native builds before upgrading.

! allow-scripts no longer matches a lower version with the allowed version — a pinned entry for an older version of a package will not cover a newer one.

! allow-scripts now defaults to pinning versions; existing configurations require a migration action to continue working.

! Node.js v18 is no longer supported.

WAS THIS USEFUL?  

Endor Labs

Feedback ⓘ

Your coding agents have a sandbox | Endor Labs (2026-11-18) BLOG ↗ RANK

Endor Labs is an application security platform built for AI-generated and human-written code, helping teams prioritize and fix real risk across the SDLC.

> Endor Labs added sandbox posture reporting to Coding Agent Governance, giving teams visibility into which developers run coding agent sessions without a sandbox and the ability to enforce sandbox use via policy.

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

01 Sandbox posture reporting in Coding Agent Governance

Not checked yet NEW 60

A new Sandboxing view in the Inventory section shows one row per developer: agents used, session count, and the share of sessions that had the sandbox on. A new Sandbox Gap widget on the Overview lists every developer below 100% sandbox coverage, surfacing who to follow up with. Sessions where sandbox state could not be determined are counted as unknown and pull a developer below 100%, distinguishing a reporting gap from a configuration gap.

Review which developers ran coding agent sessions without a sandbox and prioritize outreach by checking the Sandbox Gap widget on the Overview.

> 📍 In the Endor Labs console, go to Overview › Sandbox Gap widget to see every developer below 100% sandbox coverage, then go to Inventory › Sandboxing view to drill into per-developer session counts and coverage percentages.

— Names UI locations and coverage logic but no config/API surface

Your coding agents have a sandbox | End…

THINNER COVERAGE BELOW

02 Session policies block agentless sandbox starts

Not checked yet NEW 42

New session policies alert or block when a coding agent session starts without a sandbox enabled.

— States the mechanism but no policy config syntax given

Your coding agents have a sandbox | End…

WAS THIS USEFUL?

Cloudsmith

Feedback

API key rules are now generally available (2026-11-18) BLOG ↗ RANK

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

> Cloudsmith made API key rules generally available, letting organizations enforce separate expiration and rotation requirements for user and service accounts.

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

01 **Independent API key rules for user and service accounts**

Not checked yet NEW 60

API key rules are now generally available, allowing separate expiration and rotation requirements to be set for user accounts versus service accounts rather than a single rule applying to both — for example, rotating user keys every 30 days and service account keys every 60.

— Explains mechanism and example rotation periods but no exact config path/API.

API key rules are now generally availab…

WAS THIS USEFUL?

StepSecurity

Feedback

Harden-Runner GitHub Action v2.23.0: Secure Registry Community Tier (2026-11-18)

BLOG ↗ RANK

StepSecurity secures GitHub Actions CI/CD pipelines by detecting and preventing supply chain attacks, enforcing least-privilege permissions, and providing runtime security controls.

> StepSecurity's Harden-Runner v2.23.0 introduces Secure Registry, a community-tier feature that routes npm, npx, pnpm, and Bun 1.4.4+ installs through a protective layer that blocks malicious packages and delays new releases.

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

01 **Secure Registry for npm, npx, pnpm and Bun installs**

Not checked yet NEW 93

Setting `secure-registry: true` on the Harden-Runner GitHub Action routes npm, npx, pnpm, and Bun 1.4.4+ installs through StepSecurity's Secure Registry with no infrastructure or command changes. It always blocks package versions flagged as known-compromised or malicious by the StepSecurity SOC, and holds back newly published versions for a configurable cooldown period (0 to 30 days, default 2 days) so builds only install versions that have cleared the window. Users can add a custom block list to refuse specific packages or versions, and can inspect held/blocked versions in the job summary — which includes a ready-to-paste snippet to allow a specific held version — or review each job's package requests on the Packages tab of the StepSecurity dashboard.

Enable Secure Registry on a public repo to block compromised npm packages and apply a 7-day cooldown before new versions reach your CI build.

yaml

```yaml
- name: Harden Runner
  uses: step-security/harden-runner@v2.23.0
  with:
    secure-registry: true
```

— Names the exact flag, cooldown range/default, and dashboard tab.

Harden-Runner GitHub Action v2.23.0: Se…

WAS THIS USEFUL? 👍 👎

◆ Mobile App Security

jadx Feedback ⓘ v1.5.7 NOTES ↗ RANK

Jadx is a dex to Java decompiler

> jadx v1.5.7 adds native macOS and Windows installers alongside several GUI navigation improvements, including a richer inheritance graph and a tree filter.

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

01 **Native installers for jadx-gui** Not checked yet NEW 78

jadx-gui now ships as a macOS DMG install bundle (`jadx-gui-1.5.7-mac-aarch64.dmg` and `jadx-gui-1.5.7-mac-x86_64.dmg`) with file-type associations for macOS, and as a Windows MSI installer (`jadx-gui-1.5.7.msi`) with a bundled JRE.

– Names exact installer filenames and bundled JRE detail v1.5.7

THINNER COVERAGE BELOW

02 **GUI resource and class tree navigation improvements**

Not checked yet IMPROVED 42

The GUI ResourcePanel now uses file-type specific tabs for navigating resources, and a new tree filter was added to the GUI class/package tree for narrowing down entries.

– Describes UI changes but no exact navigation path v1.5.7

03 **Bidirectional inheritance graph in GUI** Not checked yet IMPROVED 40

Inheritance graphs in the GUI now display both super and subclass relations, not just one direction as before.

– Explains before/after behaviour but no exact UI path v1.5.7

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

PortSwigger Burp Suite

Feedback ⓘ

DAST 2026.11.2 (2026-11-18) 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's DAST module gained new scan target types for MCP servers and uploaded API definitions, while Professional/Community added an in-app Academy tab for Web Security Academy labs.

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

01 **New DAST scan targets: MCP servers and API definitions**

Not checked yet NEW 40

Burp Suite DAST can now scan MCP servers directly, and can scan uploaded API definitions at the URL where the definition is hosted.

— Names two new scan targets but no mechanism or UI path given

DAST 2026.11.2 (2026-11-18)

WAS THIS USEFUL? 👍 👎

◆ Application Security Posture

OX Security

Feedback ⓘ

Introducing OX Radar & Response Center: When News Breaks, Know If You're Affected (2026-1

BLOG ↗ RANK

OX Security is an 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 launched OX Radar and a Response Center that turn emerging supply-chain threats into actionable, trackable incidents, and added detection and mitigation guidance for the Java4Shell JVM vulnerability (CVE-2026-114938).

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

01 **Java4Shell (CVE-2026-114938) detection and mitigation**

Not checked yet NEW 92

The Issues page can be filtered by `CVE-2026-114938` to see which container images bundle a vulnerable OpenJDK runtime and how OX prioritizes each one. Exposure requires a host's CPU to have the `avx512f`, `avx512bw`, `avx512vbmi`, and `bmi2` flags, checkable via `grep -m1 '^flags' /proc/cpuinfo | tr ' ' '\n' | grep -E '^(avx512f|avx512bw|avx512vbmi|bmi2)$'`. The vulnerable JVM Base64 decoder can be disabled without affecting other AVX-512 optimizations by starting the JVM with `-XX:-UseBASE64Intrinsics`.

Identify which of your container images bundle a vulnerable OpenJDK runtime so you can prioritize rebuilds.

> 📍 In the OX Security console, go to Issues, then apply the CVE filter set to `CVE-2026-114938` to see affected images and their priority scores.

Quickly confirm whether a Linux host's CPU has all four flags required for Java4Shell RCE risk before deciding whether to patch urgently.

```
$ grep -m1 '^flags' /proc/cpuinfo | tr ' ' '\n' | grep -E
'^(avx512f|avx512bw|avx512vbmi|bmi2)$'
```

Mitigate Java4Shell on a host you cannot patch immediately by disabling only the vulnerable Base64 decoder intrinsic at JVM startup.

```
$ java -XX:-UseBASE64Intrinsics -jar your-application.jar
```

— Exact CVE filter, flag and runnable mitigation/check commands given.

Java4Shell (CVE-2026-114938): Easy to C…

---

02 **OX Radar and Response Center for threat tracking** Not checked yet

NEW DETECTION NEW INTEGRATION NEW 88

OX Radar monitors the cyber landscape in real time and marks each supply chain threat as Detected or Not Detected against your code, containers, cloud, and developer environments via the OX context lake. The Response Center turns every Radar incident into a live record with a remediation plan, open-ticket and fix-PR creation, safe-version pinning, and an audit trail, covering malicious dependencies, known exploited vulnerabilities, new CVSS 10 vulnerabilities, and reported exploits. Not Detected incidents produce shareable VEX statements and auto-close after 14 clean days of continuous monitoring, and teams can create custom incidents from an advisory URL, CVE ID, or GHSA ID under Your own incidents. A public OX Radar site lets anyone search 785K+ tracked assets — MCP servers, AI skills, npm and PyPy packages — filter by ecosystem, see risk scores, and read OX Research findings.

When a critical CVE breaks in the news, open the Response Center from the OX dashboard to see whether it is Detected in your environment and act on the generated remediation plan.

> 📍 In the OX Security platform, go to Dashboard › Response Center. Locate the auto-generated incident for the new CVE, review the Detected / Not Detected status, and click Open Ticket or Fix PR next to each affected asset to begin remediation.

Prove non-exposure to leadership for a specific advisory by creating a custom incident from an advisory URL, CVE ID, or GHSA ID and sharing the resulting VEX statement.

> 📍 In the OX Security platform, go to Response Center › Your own incidents and paste an advisory URL, CVE ID, or GHSA ID. OX builds the incident, monitors for 14 clean days, then auto-closes it and generates a VEX statement you can export and share.

— Names UI paths, data scope and VEX/14-day mechanism but no API.

Introducing OX Radar & Response Center:…

NEW VULNERABILITY CHECK OX Radar CVE and KEV catalog scanning

OX Security Launches OX Radar and Response Center to Show Companies Which Cyber Threat

BLOG ↗ LATEST STABLE

OX Security adds OX Radar and Response Center: continuous threat monitoring with ~10-minute scan cycles, automatic environment exposure checks, and a public threat research feed.

OX Radar continuously monitors emerging vulnerabilities, compromised software dependencies, and actively exploited threats, scanning approximately every 10 minutes. Not checked yet

The Response Center automatically assesses customer exposure for supported threats, providing evidence of exploitability, affected asset identification, remediation guidance, safe versions, fix pull requests, and ticket tracking. Not checked yet

Teams can initiate exposure investigations by supplying a CVE identifier, GitHub Security Advisory identifier, or advisory URL directly in the Response Center. Not checked yet

A publicly accessible OX Radar threat feed provides broader security research findings across the software and AI supply chain. Not checked yet

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

cortex-analyzers

Feedback ⓘ 3.10.5 NOTES ↗ RANK

Cortex Analyzers Repository

> Cortex-Analyzers 3.10.5 adds URL extraction to the MsgParser analyzer.

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

01 **URL extraction in MsgParser analyzer** Not checked yet IMPROVED

40

The MsgParser analyzer, now at version 3.1, extracts URLs found inside MSG files.

— Names analyzer and version but no usage detail 3.10.5

WAS THIS USEFUL? 👍 👎

osdfir-infrastructure

Feedback ⓘ

osdfir-infrastructure-2.16.0 NOTES ↗ RANK

Osdfir-infrastructure is a helm charts for running open source digital forensic tools in Kubernetes

> osdfir-infrastructure's Helm chart adds Google access token exchange support for Yeti and bumps the default Yeti version to 2.12.0.

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

01 **Google access token exchange for Yeti** Not checked yet NEW

40

Yeti now supports Google access token exchange, and the Helm chart defaults to Yeti 2.12.0.

— Names the version bump but no config key or flag given osdfir-infrastructure-2.16.0

WAS THIS USEFUL? 👍 👎

◆ Malware Analysis

CAPEv2 Feedback ⓘ changes since 2026-11-17 CODE ↗

CAPEv2 is an open-source malware sandbox that automatically executes and analyzes suspicious files to extract configurations, payloads, and behavioral indicators.

CAPEv2 adds full-duplex PCAP capture on Linux bridges, hardens SOCKS5/Tor guest routing, and surfaces NTSTATUS exit codes from short-lived Windows processes

Harden SOCKS5 and Tor guest routing by inserting `-I FORWARD 1 --source <ipaddr> -j DROP` to block non-TCP guest traffic (QUIC, raw UDP, ICMP) that previously bypassed `nat PREROUTING REDIRECT` and egressed over the host interface. Not checked yet

Track active Tor/SOCKS5 guest IPs in a new `raw` chain `CAPE_TOR_CLIENTS` (preserved across cleanup_rooter()) with per-IP add/remove rules. Not checked yet

Retain open process handles after Package.execute() so NTSTATUS exit codes (e.g., `0xC0000135` `STATUS_DLL_NOT_FOUND`, `0xC0000005` `STATUS_ACCESS_VIOLATION`) are recoverable from Windows processes that terminate inside `ntdll!LdrpInitializeProcess`. Not checked yet

WAS THIS USEFUL? 👍 👎

malcontent

Feedback ⓘ v1.28.2 NOTES ↗

Malcontent is a #supply #chain #attack #detection

malcontent now extracts cpio archives (initramfs) member by member, extending transparent archive support to this format.

└──▷ GET THIS VERSION ▾

Homebrew

```
$ brew install malcontent
# already installed? upgrade to this version:
$ brew upgrade malcontent
```

git

```
$ git clone --branch v1.28.2 https://github.com/chainguard-dev/malcontent.git
# already have the repo? check out this version:
$ git checkout v1.28.2
```

Homebrew lists this version · checked 19 Nov Wrong command?

UPDATED DETECTION Third-party YARA rule update (2026-11-17)

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

PCAPdroid

Feedback ⓘ v2.0.3 CODE ↗ RANK

PCAPdroid is a no-root network monitor, firewall and PCAP dumper for Android

> PCAPdroid v2.0.3 improves network visibility with automatic geolocation database updates and more accurate DNS resolution, alongside a new Hebrew translation.

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

01 **System DNS usage and Quad9 fallback** Not checked yet IMPROVED

40

PCAPdroid now uses the system DNS server across the entire capture session, improving DNS accuracy in VPN mode. When no system DNS server is available, it falls back to Quad9 unfiltered, replacing the previous default fallback.

— Names mechanism and before/after but no config surface v2.0.3

02 **Automatic geolocation database updates** Not checked yet IMPROVED

30

PCAPdroid now auto-updates the geolocation database used for IP-to-location lookups, so results stay current without the user manually refreshing it.

— Describes behavior but no mechanism or schedule details v2.0.3

03 **Hebrew translation added** Not checked yet NEW

25

PCAPdroid adds a Hebrew (he/iw) translation, covering all 589 UI strings and Play Store metadata.

— States scope but no user action required v2.0.3

WAS THIS USEFUL? 👍 👎

Netcap Feedback ⓘ v0.16.11 NOTES ↗ CODE ↗

Netcap is a framework for efficient, secure processing and analysis of network traffic using Go and serialized audit records.

Netcap adds offline TCP budget loss-tolerance flags, incremental HTTP decoding, MCP bounded inventory APIs, and Windows CLI signing in v0.16.11.

└──▷ GET THIS VERSION ▾

```
$ git clone --branch v0.16.11 https://github.com/dreadl0ck/netcap.git
# already have the repo? check out this version:
$ git checkout v0.16.11
```

Control TCP page-budget exhaustion during offline capture with `--local-reassembly-page-loss`, `--local-retained-payload-loss`, and `--local-completion-state-loss` flags; affected flows omit application decoding and exit with code 2. Not checked yet

Add `--incremental-http` flag (env `NC_INCREMENTAL_HTTP`) to opt HTTP/1 streams with an observed TCP handshake into bounded transaction-time decoding while leaving other protocols as completion-only. Not checked yet

UPDATED INTEGRATION Add byte-bounded inventory pages, search, matched totals, generation checks, structured field and JSON Pointer projection, and complete oversized JSON artifact delivery through the MCP server; count-only queries scan all matches without transferring record bodies. Not checked yet

Add `--pcapng-merge-sections` flag to explicitly enable compatible-interface continuity when reading PCAPNG files with multiple sections. Not checked yet

Support TLS stream following via `tshark` with automatic namespace discovery: modern `tls.stream` or legacy `tcp.stream` after an unsupported-field diagnostic. Not checked yet

+5 more

NEW SUPPORTED PLATFORM Darwin USB and new LinkFrame link types

NEW SUPPORTED PLATFORM Upper protocol profiles: BACnet, MPEG-TS, H.264/H.265/AAC, Bluetooth, USB

NEW SUPPORTED PLATFORM USB link types 189, 220, 249 in PCAP/PCAPNG

NEW SUPPORTED PLATFORM PPI/DLT 192 decoding with nested Ethernet and raw IP

└──▷ BREAKING ON UPGRADE

! The `--quiet` flag no longer authorizes overwriting existing output; noninteractive replacement now requires `-y`.

WAS THIS USEFUL? 👍 👎

◆ Firewalls & Network Defense

Humanix

Feedback ⓘ announced · Nov 17, 2026 PRESS ↗

Humanix detects and stops social engineering attacks as they unfold across email, chat, voice, and help desk workflows.

Humanix adds Complete Call Context: per-request micro-agents correlate live service-desk calls with IdP and ITSM records to detect vishing in real time.

NEW DETECTION NEW INTEGRATION Adds Complete Call Context, which spawns a micro-agent per sensitive service-desk request (such as an MFA reset or password change) to correlate call behaviour with identity provider and IT service management records, then raises a severity-rated alert with a plain-language explanation when any discrepancy or missing evidence is found. Not checked yet

Micro-agents now check caller claims against directory, ticketing, and identity provider records in real time — flagging conflicts such as a mismatched manager, a non-existent ticket number, or an unverified identity claim — rather than waiting until after the call. Not checked yet

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

Plexicus

Feedback ⓘ changelog · Nov 19, 2026 CHANGELOG ↗ RANK

Plexicus validates security findings with evidence and helps your team fix what matters. AI Swarm Pentest, Deep Code Analysis, Remediation and XBOM.

> Plexicus added finer control over AI pentest retests, letting teams cancel and inspect retests mid-run.

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

01 **Cancel and inspect AI pentest retests mid-run** Not checked yet

NEW 30

Teams can now cancel and inspect AI pentest retests while they are running, giving finer control over retest scope.

— Describes capability but no UI path or API detail changelog-20261119-a07ed549

WAS THIS USEFUL? 👍 👎

◆ CNAPP

Plerion

Feedback ⓘ

Security group rules that name a prefix list now count: NOTES ↗ RANK

Plerion is a cloud security platform that provides unified visibility, risk prioritization, and remediation across cloud environments to help organizations manage and reduce security risks.

> Plerion closed gaps in AWS security group evaluation by accounting for prefix lists and split CIDR ranges, added IPv6-aware reachability detection for EC2 instances, and introduced a check for end-of-support DocumentDB engine versions.

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

01 **IPv6-only reachability detection for EC2 instances**

Not checked yet IMPROVED 70

EC2 instance public-access check `PLERION-AWS-194` now fails instances reachable over IPv6-only paths. It reads IPv6 addresses and delegated prefixes on the network interface and counts IPv6 ACL rules in both directions.

— Named check ID and mechanism given, but no remediation step described

Security group rules that name a prefix…

02 **Prefix list and split-range detection in security group checks**

Not checked yet IMPROVED 69

Security group public-access checks now expand AWS prefix list entries and treat them as CIDR ranges, covering a customer's own prefix lists, AWS-managed lists, and cross-account shared lists — expect new failed findings on resources opened widely through a prefix list. Security group rule checks for SSH, RDP, CIFS, and other judged ports now also count prefix list entries alongside inline CIDR ranges, and treat split-range pairs such as `0.0.0.0/1` with `128.0.0.0/1` as equivalent to `0.0.0.0/0`.

— Mechanism and scope well described but no user action beyond new findings appearing

Security group rules that name a prefix…

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Huntress

Feedback ⓘ Introducing the new Security Insights Report

NOTES ↗ RANK

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

> Huntress introduced a new Security Insights Report that replaces the legacy Threat Report with richer, multi-product breakdowns, and added per-organization override controls to RMM Guard.

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

01 Per-organization RMM tool approve/reject overrides

Not checked yet NEW 85

RMM Guard now lets you approve or reject an RMM tool for a single client organization independently of the account-level decision, with the override applying only to that organization's endpoints. Use Reset to account default in an organization's RMM Guard tool drawer to revert to the account-level decision, and use the Overridden filter in the RMM Tools Inventory to list only tools with organization-level decisions, with badges like Rejected · 1 org approved showing the split. Each organization's own RMM Guard dashboard and tools inventory are accessible under ESPM in the left navigation while viewing that organization.

Override an account-level RMM tool decision for one client whose workflow depends on a tool you have blocked elsewhere.

> 📍 In the Huntress console: open the target organization › ESPM › RMM Guard › locate the tool › open its tool drawer › select Approve or Reject. The decision applies only to that organization's endpoints.

Quickly audit which RMM tools have split decisions across your client base from the account dashboard.

> 📍 In the Huntress console: go to the account-level RMM Tools Inventory › apply the Overridden filter › open any flagged tool to see per-organization decisions and Org override badges.

— Names filter, badges, drawer action and nav path precisely

RMM Guard: approve or reject RMM tools …

02 Security Insights Report replaces legacy Threat Report

Not checked yet

78

BREAKING

The new Security Insights Report covers detection and response activity, security coverage, and SOC activity, available as monthly and quarterly reports at both account and organization level from the Reports page. It adds product-level breakdowns for Managed EDR, ITDR, SIEM, and ISPM in a single report, two new EDR report pages (Firewall Status Monitoring and External Recon), a Cross-product Incident Summary page organizing every incident by severity and product, and a Standalone One-Page Summary (formerly Results Snapshot) for non-technical stakeholders. Starting March 1, 2027, the legacy Threat Report will no longer be generated, so any workflow that forwards, parses, or archives it must switch to the Security Insights Report before that date.

Find monthly or quarterly Security Insights Reports for a specific organization without waiting for the email distribution.

> 📍 In Huntress, go to Reports, select the organization from the organization selector, then open the Security Insights Report for the desired monthly or quarterly period.

— Names report pages and sunset date; access via UI path only

Introducing the new Security Insights R…

NEW INTEGRATION ConnectWise Manage PSA Response Pod

└──▷ BREAKING ON UPGRADE

! Starting March 1, 2027, the legacy Threat Report will no longer be generated; any workflow that forwards, parses, or archives the legacy report must be updated to use the Security Insights Report before that date.

Respond to Huntress incidents directly from ConnectWise tickets NOTES ↗

LATEST STABLE

Huntress adds a ConnectWise Manage PSA Response Pod letting technicians act on incidents — approve remediations, add comments, resolve escalations — from within a ConnectWise ticket.

Approve or reject remediation plans, mark manual remediations complete, add comments, and resolve incident reports and escalations directly from a ConnectWise service ticket using the new Response Pod — no switch to the Huntress portal needed. Not checked yet

The Response Pod supports both ConnectWise web and desktop clients, requires an active Huntress ConnectWise integration, and attributes every action to the signed-in technician using their existing Huntress permissions. Not checked yet

WAS THIS USEFUL? 👍 👎

Eclypsium Feedback ⓘ

Java4Shell: Patch Java, But Check the Processor First (2026-11-19) BLOG ↗

Eclypsium's infrastructure assurance platform protects mission critical hardware and detects compromised devices in enterprises and government agencies.

Eclypsium adds a detection rule for Java4Shell CPU-flag exposure and surfaces CPUID register data through its asset API for processor-based patch prioritisation.

NEW VULNERABILITY CHECK Eclypsium adds a detection rule that identifies assets whose CPUID registers expose all four processor flags (`bmi2` , `avx512f` , `avx512bw` , `avx512vbmi`) required for Java4Shell (CVE-2026-114938) to be reachable.
Not checked yet

The Eclypsium Infrastructure Assurance Platform exposes decoded Intel processor CPUID feature registers — including the four Java4Shell flags — per asset through its API, enabling automated patch prioritisation. Not checked yet

WAS THIS USEFUL? 👍 👎

XFA Feedback ⓘ Secure 1Password with XFA NOTES ↗

XFA is a developer tool that enables building fast, interactive web forms with advanced logic, validation, and data binding capabilities.

XFA adds a 1Password integration to enforce device-posture checks before SSO unlock, configured under Integrations > 1Password card > Sign-in checks.

NEW INTEGRATION Enable device-posture checks for 1Password SSO logins by navigating to Integrations, clicking Set up on the 1Password card, then Set up in the Sign-in checks section. Not checked yet

WAS THIS USEFUL? 👍 👎

Trend Vision One

Feedback ⓘ

TrendAI Vision One™ Zero Trust Secure Access module for Windows version 2.40.1049 (2026-1

BLOG ↗ RANK

Trend Vision One is a unified cybersecurity platform that provides extended detection and response (XDR) across endpoints, networks, email, and cloud environments.

> Trend Vision One's Zero Trust Secure Access module for Windows added Windows 11 26H2 compatibility and sped up Internet Access module initialization for devices with many user accounts.

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

01 **Windows 11 26H2 compatibility for ZTSA** Not checked yet IMPROVED

30

Trend Vision One ZTSA module for Windows is now verified compatible with Windows 11 version 26H2.

– States compatibility only, no mechanism or detail

TrendAI Vision One™ Zero Trust Secure A…

02 **Faster Internet Access module initialization** Not checked yet

IMPROVED

25

Internet Access module initialization now performs faster on Windows devices with many user accounts.

– Describes improvement without numbers or mechanism

TrendAI Vision One™ Zero Trust Secure A…

NEW SUPPORTED PLATFORM macOS 27 (Golden Gate) support

RETIRED SUPPORTED PLATFORM macOS 12 support dropped

TrendAI Vision One™ Zero Trust Secure Access module for macOS version 2.34.88 (2026-11

BLOG ↗ LATEST STABLE

Trend Vision One ZTSA module for macOS adds support for macOS 27 (Golden Gate); macOS 12 is no longer supported.

└──▷ **BREAKING ON UPGRADE**

! macOS 12 is no longer supported; the minimum supported macOS version is now macOS 13.

WAS THIS USEFUL?  

◆ Detection Engineering

Splunk Security Content

Feedback ⓘ v6.11.0 NOTES ↗

RANK

Splunk Security Content

> Splunk Security Content v6.11.0 adds 17 new detections and 3 new analytic stories spanning Java deserialization, Linux service-account abuse, browser cache smuggling, command-line evasion, and C2 tunneling, while splitting out a Linux-specific Sysmon macro and scheduling several legacy detections for removal.

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

01 New macros for Java and Zeek HTTP detections, Sysmon macro split

Not checked yet — 90

BREAKING

Adds 7 new macros — `sysmon_linux`, `java_hotspot_exceptions`, `java_hotspot_fatal`, `java_hotspot_jit`, `zeek_http_post_body`, `zeek_http_request_headers`, and `zeek_http_uri` — supporting new Java and Zeek HTTP detections. `sysmon_linux` separates the Linux Sysmon source `source=Syslog:Linux-Sysmon/Operational` out of the shared `sysmon` macro to avoid cross-platform event-schema collisions; the `sysmon` macro no longer includes this source, so users must update `sysmon_linux` with their sourcetype if defaults are changed or not used. This change affects the Linux Compiled C Source To Tmp and Linux Suspicious Namespace Creation detections.

— Names all macros and the affected detections and sourcetype action. v6.11.0

02 Scheduled removals of legacy detections and a story

Not checked yet DEPRECATED — 80

Windows DisableAntiSpyware Registry detection is scheduled for removal in v6.14.0; replace it with Disable Defender AntiVirus Registry. Windows Ngrok Reverse Proxy Usage detection is scheduled for removal in v6.14.0; replace it with Ngrok Reverse Proxy Usage. Windows NirSoft AdvancedRun detection is scheduled for removal in v6.12.0; replace it with Windows NirSoft Utilities. JBoss Vulnerability analytic story is scheduled for removal in v6.14.0 with no replacement.

— Names exact detections, replacements, and removal versions. v6.11.0

03 New analytic stories: Java4Shell, SSHHole, Browser Cache Smuggling

Not checked yet NEW 70

Java4Shell - CVE-2026-114938 adds detections for malformed Base64 in HTTP traffic, Base64-related JVM exceptions, and nearby Java process or file activity to connect network and host evidence. SSHHole adds Linux detections for shell execution through auditd, privilege escalation via Doas, and possible SSH bypass to improve visibility into service-account misuse. Browser Cache Smuggling adds detections for non-browser processes and PowerShell script blocks accessing browser cache directories, plus refined clipboard and browser-copy execution analytics.

— Names each story and its constituent detections, no commands given. v6.11.0

---

04 **Detections for native-messaging abuse, command-line evasion, tunneling, and persistence**

Not checked yet NEW 70

New detections cover native messaging hosts registered by user-writable binaries and native messaging hosts that spawn user-writable processes; evasive Windows command-line patterns including native-command chaining, encoded character sequences, and superscript character obfuscation; Ngrok reverse proxy usage and BITS upload activity, alongside refined BITS, Ngrok, and Cloudflared analytics; and Run key self-registration from user-writable paths.

— Names several distinct detection targets but no exact query names. v6.11.0

THINNER COVERAGE BELOW

05 **Updated Windows Certificate Services analytic story**

Not checked yet IMPROVED 25

The Windows Certificate Services analytic story was updated to keep certificate-services detection coverage current.

— Bare mention with no detail on what changed. v6.11.0

└──▷ **BREAKING ON UPGRADE**

! The `sysmon` macro no longer includes the Linux Sysmon source `source=Syslog:Linux-Sysmon/Operational`; that definition now lives in the new `sysmon_linux` macro, which must be updated with your sourcetype. The two detections affected are Linux Compiled C Source To Tmp and Linux Suspicious Namespace Creation.

! Windows DisableAntiSpyware Registry detection is scheduled for removal in v6.14.0; replace it with Disable Defender AntiVirus Registry.

! Windows Ngrok Reverse Proxy Usage detection is scheduled for removal in v6.14.0; replace it with Ngrok Reverse Proxy Usage.

! Windows NirSoft AdvancedRun detection is scheduled for removal in v6.12.0; replace it with Windows NirSoft Utilities.

! JBoss Vulnerability analytic story is scheduled for removal in v6.14.0 with no replacement.

WAS THIS USEFUL?  

DePalma Research AI DFIR Toolkit

Feedback ⓘ

artifacts-v1.2.0 NOTES ↗ RANK

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

> AI DFIR Toolkit's artifacts-v1.2.0 release adds a Hunts tab with downloadable IOC feeds, a credential-safe host-verification script, staleness tracking for catalog entries, six new Sigma rules for Entra app abuse and SSH tunnels, four Wave 3 catalog entries, a case-study authoring skill, and a hardening section in the guide.

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

01 **IOC export feeds and per-case download buttons** Not checked yet

NEW 85

Export case-study indicators via two new API feeds: `docs/api/iocs.csv` (every indicator with description) and `docs/api/iocs/<case-id>.txt` (atomic indicators, refanged, one per line); each case also gains Copy values, Download .txt, and Download .csv buttons.

— Exact endpoint paths and formats, directly usable artifacts-v1.2.0

02 **Six new Sigma detection rules for Entra and SSH tunnels**

Not checked yet NEW 85

Adds six new Sigma rules: in `08-agentic-orchestration/`, `entra_role_member_added_by_app.yml` (directory role assigned by an app, PIM filtered), `entra_app_credential_added_by_app.yml` (secret or certificate added to an app by an app), `artex_default_probe_file_created.yml` (default ARTEX framework file on a target), `entra_app_signin_invalid_or_expired_secret.yml` (Entra app sign-in failing with wrong or expired client secret), and `entra_app_signin_scripted_client.yml` (successful app sign-in from a bare scripting client, both reading the service principal sign-in log); plus `reverse_ssh_tunnel_exposing_local_sshd.yml` in `artifacts/detections/sigma/` (tunnel opened by tampered editor extension of AIRT-CS-0023); the pack is now 76 rule files / 171 signatures.

— Every rule file named with exact behaviour and pack totals artifacts-v1.2.0

03 **Host verification script for live-host artifact checks**

Not checked yet NEW 80

New `scripts/verify_host.py` and `docs/HOST_VERIFICATION.md` let practitioners stat artifact paths on a live host without opening files or leaking credentials; a MISS is always reported as a miss, never a wrong path.

— Named script and doc path, clear safety guarantee stated `artifacts-v1.2.0`

---

04 **Hunts tab aggregating Sigma rules and indicators** Not checked yet

NEW

75

New Hunts tab on the site lists Sigma rules at low level and all `behavior` indicators from case studies, grouped by case, with permalinks, filters, and copy-as-Markdown-checklist; anchors and cross-references are gated by `build_site.py --check`.

— Names tab, gating flag and UI affordances but no counts `artifacts-v1.2.0`

---

05 **Wave 3 catalog entries for agent tooling** Not checked yet NEW

75

Adds four Wave 3 catalog entries: `AIRT-0046` Warp, `AIRT-0047` Letta, `AIRT-0048` Docker Model Runner, and `AIRT-0049` agent framework libraries (Semantic Kernel, PydanticAI, Smolagents, OpenAI Agents SDK, Strands), inventoried by dependency manifest, site-packages presence, process lineage, and provider egress.

— Named entries and inventory signals, no direct action step `artifacts-v1.2.0`

---

06 **Catalog staleness tracking via last_verified field**

Not checked yet IMPROVED

70

Adds `last_verified` field to catalog entries and staleness reporting against a 90-day cadence; `validate.py` names entries never checked rather than letting them appear fresh.

— Names field, cadence and validator but no run instructions `artifacts-v1.2.0`

---

07 **Case-study authoring skill** Not checked yet NEW

70

Adds a case-study authoring skill at `skills/case-study-authoring/SKILL.md` covering indicator workflow, actor links, `basis` and `contested` fields, and a six-question audit for existing cases.

— Named file and fields but audit content unspecified `artifacts-v1.2.0`

---

08 **Hardening section injected into guide** Not checked yet NEW

65

Adds a hardening section in the guide injected at `<!-- site:hardening -->` with counts of plaintext credential locations, MCP config files, and unauthenticated listeners, plus the `harden` step from every case that records one.

— Named injection anchor and metrics, no usage walkthrough `artifacts-v1.2.0`

WAS THIS USEFUL?  

◆ Threat Intelligence

MISP

Feedback ⓘ v2.5.52 NOTES ↗ RANK

MISP is an open-source threat intelligence platform that enables organisations to share, store, and correlate indicators of compromise and cybersecurity threat data.

> MISP 2.5.52 adds cross-version sync between 2.5 and 3.x instances, misp-modules feed gathering with per-module timeouts, and encrypted OIDC refresh tokens, alongside a major security-hardening pass covering trusted-proxy IP resolution, decompressed payload caps, and the removal of several legacy endpoints, importers and the Python 3.10 toolchain.

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

01 Trusted proxy configuration for client IP resolution

Not checked yet 90

BREAKING

The new `MISP.trusted_proxies` setting lets admins declare which reverse proxies are trusted, used for auth key IP restrictions, brute-force protection, and logs. This changes existing behaviour: when `MISP.log_client_ip_header` is set, MISP now reads the client address from the trusted (right-most) end of the header instead of the left-most, so multi-proxy deployments must list every proxy in `MISP.trusted_proxies` to keep IP resolution correct.

Register the proxy chain so MISP resolves the correct client IP for auth key restrictions and brute-force protection when sitting behind two reverse proxies.

ini

```
MISP.trusted_proxies = ['10.0.0.1', '10.0.0.2']
```

— Exact config key, header behaviour change, and runnable example. v2.5.52

02 Decompressed payload size cap and compression restrictions

Not checked yet 90

BREAKING

The new `Security.max_decompressed_size` setting caps decompressed request and feed/sync response sizes. Compressed bodies are now only decoded for authenticated users and only over gzip; brotli and zstd are no longer accepted.

Prevent memory exhaustion when ingesting large feeds or sync responses by capping the decompressed payload size.

```ini
Security.max_decompressed_size = 536870912
```

— Named setting plus concrete before/after on accepted encodings. v2.5.52

03 **Python 3.11 requirement** Not checked yet BREAKING 85

MISP's Python environment now requires Python 3.11 or newer; PyMISP 3.0.0 and the matching misp-stix release no longer install on Python 3.10. Ubuntu 22.04 users must install a newer Python, rebuild the virtual environment, and point `MISP.python_bin` at the new interpreter.

— Exact migration steps and config key given. v2.5.52

04 **Encrypted OIDC refresh tokens** Not checked yet NEW 80

OIDC refresh tokens are now stored encrypted when `Security.encryption_key` is set; existing plaintext tokens remain functional.

Encrypt OIDC refresh tokens at rest so that tokens stored in the database are not readable as plaintext.

```ini
Security.encryption_key = '<your-32-byte-or-longer-key>'
```

— Exact config key and runnable example value provided. v2.5.52

05 **Password reset email requires configured base URL** Not checked yet 70

BREAKING

Password reset e-mails are only sent when `MISP.baseurl` or `MISP.external_baseurl` is configured; MISP no longer builds the reset link from the request's `Host` header.

— Named config keys with clear before/after. v2.5.52

06 **misp-modules feed gathering and per-module timeouts**

Not checked yet NEW 65

misp-modules gathering modules can now be used as a feed source: the module produces a standard MISP feed streamed through the existing feed importer, with setup documented in `design-doc/misp-modules/gathering-feeds.md`. Per-module execution timeouts can also be set for misp-modules.

— Groups two thin misp-modules additions with a named doc path. v2.5.52

07 **Overmind interface UI enhancements** Not checked yet IMPROVED

65

The Overmind interface gains a Timeline tab and galaxy matrix card in the event view, an Ownership & Distribution card, IDs and UUIDs in the page header, a zoom and filter mode for the correlation graph, a reworked REST client, entity extraction when editing a report, and bulk hard and soft deletes on the attribute, object, and galaxy cluster indexes.

— Many named UI additions but little mechanism per item. v2.5.52

---

08 **MISP 2.5 to 3.x cross-version sync** Not checked yet NEW

60

MISP 2.5 instances can now sync with MISP 3.x instances, with version-dependent features such as proposals, organisation rules, protected events, and sighting searches remaining available against a 3.x remote.

— Lists preserved features but no setup or config steps. v2.5.52

---

09 **STIX sightings endpoint and legacy STIX 1 importer removed**

Not checked yet DEPRECATED

60

The STIX sightings upload endpoint `POST /sightings/add/stix` has been removed, and the legacy STIX 1 importer has been removed; STIX 1 imports now go through misp-stix.

— Named endpoint and replacement import path given. v2.5.52

THINNER COVERAGE BELOW

10 **CertAuth requires server-verified client certificates**

Not checked yet BREAKING

55

CertAuth now only accepts client certificates that the web server has verified, requiring `SSL_CLIENT_VERIFY=SUCCESS`.

— Names the verification flag but limited further detail. v2.5.52

---

11 **Event restore/recover endpoints removed** Not checked yet

DEPRECATED

55

The `events/restoreDeletedEvents` and `events/recoverEvent` endpoints and their CLI command have been removed.

— Named endpoints but no replacement path given. v2.5.52

---

12 **Login e-mail changes restricted under external auth**

Not checked yet BREAKING

45

While external authentication (LDAP, Shibboleth, or other backends) is configured, only site admins can change a user's login e-mail.

— Clear rule but no config surface or endpoint named. v2.5.52

---

13 **GnuPG host-org signing restriction setting removed**

Not checked yet DEPRECATED 35

The `GnuPG.restrict_server_signing_to_host_org` setting has been removed.

— Bare removal notice with no replacement detail. v2.5.52

└──▷ **BREAKING ON UPGRADE**

! Python 3.11 or newer is now required for MISP's Python environment; PyMISP 3.0.0 and the matching misp-stix release no longer install on Python 3.10. Ubuntu 22.04 users must install a newer Python, rebuild the virtual environment, and point `MISP.python_bin` at the new interpreter.

! When `MISP.log_client_ip_header` is set, MISP now takes the client address from the trusted (right-most) end of the header rather than the left-most; multi-proxy setups must list all proxies in the new `MISP.trusted_proxies` setting to maintain correct IP resolution for auth key restrictions, brute-force protection, and logs.

! Password reset e-mails are only sent when `MISP.baseurl` or `MISP.external_baseurl` is configured; MISP no longer builds the reset link from the request's `Host` header.

! CertAuth now only accepts client certificates that the web server has verified with `SSL_CLIENT_VERIFY=SUCCESS`.

! Compressed request bodies (and feed/sync responses) are only decoded for authenticated users, gzip only; brotli and zstd are no longer accepted.

! While external authentication (LDAP, Shibboleth, or other backends) is configured, only site admins can change a user's login e-mail.

! The `events/restoreDeletedEvents`, `events/recoverEvent` endpoints and their CLI command have been removed.

! The STIX sightings upload endpoint `POST /sightings/add/stix` has been removed.

! The legacy STIX 1 importer has been removed; STIX 1 imports now go through misp-stix.

! The `GnuPG.restrict_server_signing_to_host_org` setting has been removed.

WAS THIS USEFUL? 👍 👎

Cyberbro

Feedback ⓘ v0.16.0 NOTES ↗

Cyberbro is an open-source threat intelligence tool that analyzes indicators of compromise (IPs, hashes, URLs, domains) across multiple security services simultaneously.

└──▷ GET THIS VERSION ▾

Docker

```
$ docker pull ghcr.io/stanfrbd/cyberbro:v0.16.0
```

git

```
$ git clone --branch v0.16.0 https://github.com/stanfrbd/cyberbro.git
# already have the repo? check out this version:
$ git checkout v0.16.0
```

published under the project's GitHub account · checked 19 Nov Wrong command?

NEW DETECTION VPNDetection engine

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines

Feedback ⓘ New sidebar for saved views in Cases (2026-11-18)

BLOG ↗ RANK

Tines is an apps, agents and automations, in the complete environment for enterprise AI.

> Tines added a dedicated sidebar in Cases for quickly switching between saved views.

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

01 Saved views sidebar in Cases

Not checked yet IMPROVED

40

Cases now has a dedicated sidebar that lists all saved views at a glance, letting users switch between them in one click instead of opening the dropdown next to the search filters.



Switch between saved case views without opening a dropdown — the sidebar surfaces them all at once.

> 📍 In Cases, open the sidebar panel on the left to see all saved views listed, then click any view to switch to it instantly.

— Clear UI change and navigation path, but no deeper mechanism.

New sidebar for saved views in Cases (2…

WAS THIS USEFUL? 👍 👎

◆ SIEM

Databricks

Feedback ⓘ

Configurable retention for system tables is generally available (2026-11-18)

BLOG ↗ RANK

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

> Databricks brought the Lakebase streaming sink to general availability with native PostgreSQL writes and schema evolution, alongside GA configurable retention for system tables, new Unity Catalog service policies for AI Gateway (streaming output evaluation and embedding input protection), a per-recipient TTL control for OpenSharing, and a fix letting Lakewatch rules be tested against historical data.

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

01 Lakebase streaming sink reaches GA with Postgres writes

Not checked yet NEW INTEGRATION IMPROVED 90

The Lakebase streaming sink is now generally available, writing to an external PostgreSQL database through a Unity Catalog connection. It supports merge strategies and additive schema evolution via `mergeSchema` on Databricks Runtime 19 and above, and now supports Trigger.AvailableNow() on serverless jobs and notebooks.

— Names exact config key, trigger method, runtime version and connection type

Lakebase streaming sink is generally av…

02 Historical time-range testing for Lakewatch detection rules

Not checked yet IMPROVED 80

On the Lakewatch query page, TIMERANGE_NOW() now returns the end of the selected time range instead of the current time, letting you test a detection rule's predicates against historical data by selecting a historical time range and using TIMERANGE_NOW() as the window boundary.

Replay a past time window in Lakewatch to verify that a detection rule fires on historical data rather than live events.

> 📍 In the Lakewatch query page, select a historical time range, then write your detection predicate using TIMERANGE_NOW() as the window boundary — it will resolve to the end of your selected range, not the current clock time.

— Names exact function and gives runnable testing steps

TIMERANGE_NOW() on the Lakewatch query …

03 Streaming evaluation default for model output policies

Not checked yet · NEW INTEGRATION · BREAKING · 65

Unity Gateway service policies for model outputs now default to streaming evaluation, releasing text without buffering or recall; select Full response evaluation to buffer the entire response before release instead. This changes existing policies' behavior — previously buffered responses are no longer held until completion unless that option is explicitly selected.

— Names the exact UI option and describes the behavior change

Evaluate streaming responses incrementa…

04 Configurable retention for system tables

Not checked yet · NEW · 62

Account-wide retention period is configurable from 30 to 3,650 days for supported system tables, now generally available; the first 395 days are free with storage charges applying beyond that threshold.

— Gives concrete numeric range and pricing but no exact setting name

Configurable retention for system table…

05 Service policies for embedding inputs

Not checked yet · NEW · 60

Service policies can now be applied to single or batch embedding inputs to mask sensitive data, deny requests containing it, or reject unsafe content before the model runs, available as a Beta capability in Unity Gateway.

— Clear description of mechanism but no API or flag named

Service policies protect embedding inpu…

THINNER COVERAGE BELOW

06 Per-recipient materialization TTL for OpenSharing

Not checked yet · NEW · 50

Set a materialization time-to-live (TTL) for individual Delta Sharing OpenSharing recipients, overriding the metastore-level default TTL.

— Describes override but no exact config field or command named

Configure materialization TTLs for indi…

└──▷ BREAKING ON UPGRADE

! Existing model output policies now default to streaming evaluation; previously buffered responses are no longer held until completion unless Full response evaluation is explicitly selected.

JDBC Unity Catalog connections are now available by default for workspaces with the co

BLOG ↗ STABLE

Databricks adds JDBC Unity Catalog connections, with SSL certificate support, as a default capability for compliance security profile workspaces.

OpenAI GPT-6.2 Astra and Sol are now available on Unity Gateway (2026-11-17)

BLOG ↗ STABLE

WAS THIS USEFUL? 👍 👎

Elastic Security Labs Feedback ⓘ

We caught the agent-framework PyPI compromise six minutes after it published (2026-11-18)

BLOG ↗

Elastic Security Labs is a powered by Elasticsearch. Ready to deploy your data?

NEW DETECTION Elastic Defend detection rules for agent-framework PyPI supply-chain compromise

NEW DETECTION ECS hunting queries for agent-framework stealer file artifacts and DNS exfiltration

WAS THIS USEFUL? 👍 👎

ClickHouse

Feedback ⓘ announced · Nov 17, 2026 BLOG ↗

ClickHouse is an open-source columnar database management system designed for fast analytical queries on large volumes of data in real time.

ClickHouse Cloud adds linked billing for Claude Platform orgs, routing Claude API charges directly to an existing Claude account with no API key required.

NEW INTEGRATION Link a Claude Platform organization to ClickHouse Cloud via Organization settings > Link your Claude organization so Anthropic bills Claude API usage directly to your Claude organization, with no API key to manage. Not checked yet

Set a monthly spend limit when linking, or change it at any time in the Claude Console, with your organization-wide Claude limit also enforced. Not checked yet

Review the connection or unlink at any time under Linked platforms in the Claude Console or Organization settings in ClickHouse Cloud. Not checked yet

└─▷ BREAKING ON UPGRADE

! While linked billing is enabled, ClickHouse Cloud serves Claude models only.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Security Validation (BAS & Automated Pentest)

Horizon3 NodeZero

Feedback ⓘ changelog · Nov 19, 2026

CHANGELOG ↗ RANK

Horizon3 NodeZero is a horizon3.ai enables organizations to continuously assess the security posture of their enterprise across many attack surfaces.

> Horizon3 NodeZero added AI-driven web app risk exploration, new login techniques for SSL VPNs and identity-gated portals, and a Risk Assessment with Safety Overrides workflow for flagging and acting on risky routes.

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

01 **Risk Assessment and Safety Overrides for risky routes**

Not checked yet NEW 55

NodeZero adds Risk Assessment and Safety Overrides features to identify potentially risky routes for blocking or targeted testing, surfaced on the Rapid Response Details page with an Asset Breakdown, a Relevant Assets table of exploitable assets, and a Take Action flow to run Rapid Response tests, add notes, or create tickets.

— UI workflow shown in screenshots but no config keys named changelog-20261119-c006200e

02 **SSL VPN and identity-gated portal login support** Not checked yet

NEW 45

NodeZero now supports SSL VPNs and identity-gated portals as target-app login techniques, with persistent authenticated session maintenance.

— Names concrete login targets but no setup steps changelog-20261119-c006200e

03 **AI agent-driven web application risk exploration** Not checked yet

IMPROVED 30

NodeZero now uses AI agents, constrained by guardrails, to more thoroughly explore and verify web application risks.

— Describes mechanism but no config or scope detail changelog-20261119-c006200e

WAS THIS USEFUL? 👍 👎

◆ Endpoint Management (UEM/RMM)

Kaseya VSA

Feedback ⓘ VSA 10: Version 10.30 release notes

NOTES ↗ RANK

Kaseya VSA is a manage more endpoints with less manual work using Datto RMM. Automate monitoring, patching, remediation and remote support while connecting IT workflows.

> Kaseya VSA 10.30 focuses on Android MDM, adding managed configuration variables, token-based enrollment, and expanded Play Store access, alongside mobile app Quick Actions and a redesigned device filter menu.

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

01 Play Store Mode for Company Owned devices

Not checked yet NEW

65

Enable all Google Play apps for Company Owned devices by toggling the `Android System Configuration > System Configuration > Play Store Mode` setting in device profiles.

Allow a Company Owned Android device to access the full Google Play catalogue rather than a curated subset.

> 📍 In the device profile editor, go to Android System Configuration › System Configuration › Play Store Mode and enable the setting.

— Names the exact config path and toggle VSA 10: Version 10.30 release notes

02 Enrollment token for Android devices without QR scanning

Not checked yet NEW

60

Enroll devices that cannot scan a QR code using the enrollment token now displayed on the MDM Enrollment page. Admins copy the token from the MDM Enrollment page and enter it manually during enrollment.

Enroll a corporate Android device that has no camera and cannot scan a QR code by supplying the token shown on the enrollment page.

> 📍 Navigate to Android MDM › MDM Enrollment page, copy the enrollment token displayed, and enter it manually on the device during the enrollment flow.

— Includes exact navigation and entry steps VSA 10: Version 10.30 release notes

THINNER COVERAGE BELOW

03 Redesigned Add Filter menu on Device Management page

Not checked yet IMPROVED 55

Find and manage device filters faster on the Device Management page with a redesigned Add Filter menu featuring submenus for Status, Device type, Context, Device attributes, and MDM Status, plus quick filtering from the Devices table.

— Names submenu categories but no exact navigation steps

VSA 10: Version 10.30 release notes

04 **Managed configuration variables in Android MDM profiles**

Not checked yet NEW 50

Define per-app variables — such as email address, organization name, or device serial number — inside Android MDM application profiles using managed configuration variables.

— Names the feature and example variables but no setup steps

VSA 10: Version 10.30 release notes

05 **Quick Actions in VSA mobile app** Not checked yet NEW 50

Perform Terminal or Remote Desktop sessions from the mobile app without navigating multiple screens by long-pressing any device in the Computer List to open Quick Actions.

— Describes the gesture but no deeper session detail VSA 10: Version 10.30 release notes

WAS THIS USEFUL?  

N-able N-central Feedback ⓘ

One patch policy experience, now across Windows, macOS, and Linux (2026-11-18)

BLOG ↗

N-able N-central is a secure endpoints and automate IT operations at scale. N-central delivers unified endpoint management with advanced RMM capabilities for complex environments.

N-able N-central adds Windows patch policies with per-classification approval rules, default future-app rules, and registry-based Windows Update access controls.

NEW SUPPORTED PLATFORM Set approval rules for Microsoft update classifications — Security Updates, Critical Updates, and Update Rollups — alongside supported third-party applications in a single Windows patch policy. Not checked yet

Set a default approval rule so future applications added to the supported catalogue automatically inherit your chosen rule without revisiting policies. Not checked yet

Control what users can see and do in Windows Update via registry key controls, including restricting user-initiated installs when patching is centrally managed. Not checked yet

└─▷ **BREAKING ON UPGRADE**

! The new Windows patching engine is separate from the existing Patch Management engine and does not use or change current Patch Management settings; running both engines on the same asset simultaneously is not recommended, as conflicting schedules, approvals, and reboot settings can cause inconsistent scan results, failed installations, and unnecessary reboot attempts.

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 expanded its Auto Apps catalog with new automated deployment support across Windows and macOS.

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

01 **New Windows and macOS Auto Apps** Not checked yet

NEW SUPPORTED PLATFORM NEW 55

Iru added automated deployment support for new Windows Auto Apps — `ChatGPT`, Mullvad VPN, Podman Desktop, Windscribe, Yealink USB Connect, `ZeroTier One`, and Zoom Outlook Plugin — available to all Endpoint customers, plus Cinema 4D 2026 as a new macOS Auto App in the Library Items catalog available to all customers.

— Names every app added but no mechanism beyond catalog listing. New Windows Auto Apps

New macOS Auto App: Cinema 4D 2026

> New macOS Auto App: Antigravity IDE NOTES ↗ STABLE

WAS THIS USEFUL? 👍 👎

◆ Vulnerability & Exposure Management

defectdojo

Feedback ⓘ 3.5.201 NOTES ↗ RANK

Defectdojo is an open-source Unified Vulnerability Management, DevSecOps & ASPM

> DefectDojo's latest release focuses on import-time asset enrichment, a new deduplication plugin hook, and a tag-lookup performance fix for bulk imports.

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

01 **CPE location emission from import formats** Not checked yet NEW

52

DefectDojo now emits CPE locations from `CycloneDX` , `SPDX` and `Dependency-Check` imports, automatically populating asset location data from these scan formats.

— Names three import formats but no exact field or command. 3.5.201

02 **Faster tag lookups during bulk import** Not checked yet IMPROVED

50

Tag lookups during bulk import now use UPPER(name) matching, avoiding full table scans on large tag sets.

— Names the exact matching mechanism but no runnable action. 3.5.201

03 **Dedupe plugin hook to protect findings** Not checked yet NEW

47

A new plugin hook in the deduplication engine lets a dedupe plugin keep specific duplicates out of the Delete Duplicates process and hold an asset, preventing them from being removed in bulk deletion.

— Describes mechanism but no concrete plugin API or config shown. 3.5.201

WAS THIS USEFUL? 👍 👎

◆ Patch Management

Automox

Feedback ⓘ

Define Patch Compliance Your Way and Configure Your Home Dashboard (2026-11-18)

BLOG ↗ RANK

Automox is a check out our full list of release notes, and stay up to date with what

> Automox introduced a configurable Home Dashboard and a new Patch Compliance widget that lets organizations define their own SLA-based compliance rules, along with matching changes to device filtering.

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

01 Patch Compliance widget with custom SLAs

Not checked yet BREAKING

76

A new Patch Compliance widget replaces the previous Policy Compliance widget, showing the percentage of devices meeting an organization-defined compliance standard rather than just scheduled-policy status. Organizations can set patch SLAs by severity, add exceptions for groups or tags, configure a new device grace period, choose whether third-party patches and disconnected devices count toward compliance, and preview changes in real time with Live Preview before saving. Because the measurement basis changed, compliance figures will likely differ from what the old Policy Compliance widget reported.

Define a custom patch compliance SLA before committing, so you can see the impact on your compliance score without affecting live data.

> 📍 In the Patch Compliance widget settings, set patch SLAs by severity, add group or tag exceptions, configure a new device grace period, and toggle third-party patch and disconnected device inclusion. Use Live Preview to see the resulting compliance percentage, then save when satisfied.

— Mechanism and before/after explained, but setup is UI-driven, no flags.

Define Patch Compliance Your Way and Co…

02 Configurable Home Dashboard layout

Not checked yet NEW

68

The Home Dashboard now lets you rearrange, resize, and hide widgets using mouse or keyboard, with the layout saved per organization. Widgets such as Available Updates, Policies Executed, and New Devices can be customized via a pencil-icon edit mode.

Configure the Home Dashboard to surface the panels your team checks daily and hide irrelevant widgets.

> 📍 In the Home Dashboard, select the pencil icon, then drag widgets to your preferred order, resize the Available Updates, Policies Executed, or New Devices widgets as needed, and hide any widgets that do not apply. Your layout is saved automatically per organization.

— Clear UI steps given, but no config key or API named.

Define Patch Compliance Your Way and Co…

03 **Devices page compliance filtering updates** Not checked yet

68

BREAKING

The Devices page gained a new Compliance column and a Non-Compliant filter showing which devices fail the organization's compliance definition and why, letting users drill from a non-compliant count on the dashboard straight to the affected devices. The existing `Compliant` filter was renamed to `Up to Date` to reflect that it now only shows devices current with their scheduled policies; saved views or workflows referencing `Compliant` need to be updated.

Drill from a non-compliant count directly to the specific devices that need patching.

> 📍 On the Home Dashboard, select the non-compliant device count in the Patch Compliance widget to open the Devices page pre-filtered to non-compliant devices, then use the Compliance column to identify which patches pushed each device out of SLA.

— Names exact filter rename and column, but no API/config surface.

Define Patch Compliance Your Way and Co…

└──▷ **BREAKING ON UPGRADE**

! The `Compliant` filter on the Devices page has been renamed to `Up to Date`; saved views or workflows referencing `Compliant` will need to be updated.

! The Patch Compliance widget measures whether every available patch was installed within your SLA, replacing the previous Policy Compliance widget which measured whether devices were up to date with scheduled policies — compliance figures will likely differ from before.

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

JumpCloud

Feedback ⓘ Release Notes 2026 (2026-11-19) 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 latest release automates access revocation and suspension when Access Certification decisions are finalized or deadlines expire, adds a tamper-proof certification export flow, introduces Agent Delegated Access token exchange, new Windows and Apple device management policies, a Directory Insights SIEM integration API, and per-application SCIM group name overrides.

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

01 Access Certification campaign export with audit trail

Not checked yet NEW 90

Admins can open a completed Access Certification campaign in the Admin Portal, select Export, choose CSV, JSON, or PDF format, and complete an administrator sign-off flow to download a tamper-proof snapshot secured with SHA-256 document hashing.

Review and export a completed access-certification campaign snapshot for a compliance audit with SHA-256 integrity verification.

📍 In the Admin Portal, go to Access Certification, open a completed campaign, and select Export. Choose CSV, JSON, or PDF as the format, then complete the administrator sign-off flow to download the tamper-proof snapshot with SHA-256 document hashing.

— Exact UI steps, formats, and hashing mechanism given. Release Notes 2026 (2026-11-19)

02 Per-application SCIM group display name override

Not checked yet NEW 88

In an SSO application's User Groups and Agent Groups tab, admins can override a SCIM group's display name per application using Show In App As, then click Save and sync to push the override immediately, keeping internal JumpCloud group names unchanged while apps receive their expected names.

Override a SCIM group's display name per application so internal JumpCloud group names stay unchanged while apps receive their expected names.

📍 In the Admin Portal, open the SSO application, go to the User Groups and Agent Groups tab, locate the group, enter the target name in Show In App As, then click

Save and sync to push the override immediately.

— Exact field name, button, and tab location given. Release Notes 2026 (2026-11-19)

03 **Directory Insights SIEM Integration API with OCSF normalization**

Not checked yet NEW 75

SIEM collectors can continuously pull JumpCloud identity events through the Directory Insights SIEM Integration API endpoint, authenticating with an existing JumpCloud API key, setting format to OCSF and output to JSON, to receive normalized identity events for real-time threat detection.

Pull JumpCloud identity events continuously into a SIEM in OCSF-normalized JSON format for real-time threat detection.

📍 Configure your SIEM collector to call the Directory Insights SIEM Integration API endpoint using your existing JumpCloud API key, with format set to OCSF and output as JSON to receive normalized identity events.

— Names endpoint, auth, and format but not exact URL. Release Notes 2026 (2026-11-19)

04 **Unified Apple device restrictions policy** Not checked yet NEW 68

Admins can manage Apple device restrictions for macOS and iOS/iPadOS from a single Restrictions policy under `Device Management > Policy Management`, covering system settings, privacy, biometrics, iCloud, and Apple Intelligence & Siri.

— Exact navigation path and setting categories given. Release Notes 2026 (2026-11-19)

THINNER COVERAGE BELOW

05 **User-level custom Windows MDM policy via OMA-URI** Not checked yet NEW 55

A new User Level Custom Windows MDM (OMA URI) Policy lets admins configure custom MDM settings scoped to a user's profile on MDM-enrolled Windows devices.

— Policy type named but no navigation path or example given.

Release Notes 2026 (2026-11-19)

06 **Agent Delegated Access token exchange** Not checked yet NEW 45

Configure allowed audiences and exchange trusted user identity tokens for signed tokens representing an agent acting on a user's behalf via Agent Delegated Access.

— Mechanism named but no concrete config path or command. Release Notes 2026 (2026-11-19)

07 **Automated access revocation on certification deadlines**

Not checked yet NEW 40

When an Access Certification review decision is finalized or a review deadline expires, JumpCloud can automatically revoke access or suspend the affected identity.

— Describes outcome but no config steps or triggers named.

Release Notes 2026 (2026-11-19)

---

08 **Workflow templates in Workflows UI** Not checked yet NEW

10

Screenshots show new template support added to the Workflows UI, illustrating how templates work, but no written description accompanies them.

— Only a screenshot caption, no written description. Release Notes 2026 (2026-11-19)

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

1Password

Feedback ⓘ

1Password for Android beta 8.12.48-24 (2026-11-18) BLOG ↗ RANK

All the latest releases from the 1Password team

> This window's shared 8.12.48-24 beta release rolled a common set of changes across every 1Password platform: a new setting to silence the can't-autofill warning, Steam Guard one-time-password support, and removal of Anti-Peek Mode (a breaking change on Android and iOS) — alongside browser-extension additions like a repositionable universal sign-in prompt, exact-host login matching for non-standard ports, and new DuckDuckGo support on Windows.

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

01 Setting to suppress can't-autofill warning

Not checked yet NEW

70

A new toggle stops the warning shown when saving a login that can't be autofilled: open `Settings > General` and turn off 'Warn when saving a login that can't be autofilled'. This setting rolled out across Android, Linux, Mac, Windows and iOS betas.

Stop 1Password from prompting a warning every time you save a login on a site it can't autofill into.

> 📍 Settings › General › turn off 'Warn when saving a login that can't be autofilled'

Silence the `can't autofill` warning that appears every time you save a login for a site that 1Password cannot autofill into.

> 📍 Open Settings › General and turn off 'Warn when saving a login that can't be autofilled'.

Suppress the autofill-warning dialog that fires every time you save a login 1Password cannot autofill — useful in environments with many internal apps.

> 📍 Open Settings › General and turn off 'Warn when saving a login that can't be autofilled'.

Turn off the autofill-warning noise when saving logins that 1Password cannot autofill, to reduce alert fatigue during bulk imports or unusual site setups.

> 📍 Settings › General › turn off 'Warn when saving a login that can't be autofilled'

Silence the can't be autofilled popup that appears every time you save a login for an app or site that doesn't support autofill.

> 📍 Settings › General › turn off 'Warn when saving a login that can't be autofilled'

— Exact settings path given, but no mechanism beyond the toggle

1Password for iOS beta 8.12.48-24 (2026… | 1Password for Windows beta 8.12.48-24 (… | 1Password for Mac beta 8.12.48-24 (2026… | 1Password for Linux beta 8.12.48-24 (20… | 1Password for Android beta 8.12.48-24 (…

---

02 **Repositionable universal sign-in prompt** Not checked yet NEW

70

The universal sign-in prompt can now be positioned at the bottom of the page by opening the browser extension's `Settings > 'Appearance & shortcuts'` and setting Universal sign-in position to Bottom; the control for this has also moved to that panel.

Move the universal sign-in prompt to the bottom of the page so it doesn't obscure page headers on login forms.

> 📍 In the browser extension, go to Settings › Appearance & shortcuts and set Universal sign-in position to Bottom.

— Exact setting name and location given with steps

1Password in the browser 8.12.48-24 (20…

---

03 **Keyboard shortcuts settings category** Not checked yet IMPROVED

60

All keyboard shortcuts now live in their own category, found via `Settings > Keyboard Shortcuts`, positioned between Browser and Developer, instead of being scattered across other panels.

Locate and customise all keyboard shortcuts from one place instead of hunting through unrelated settings panels.

> 📍 Open Settings › Keyboard Shortcuts (between the Browser and Developer categories).

Find and customise keyboard shortcuts without hunting through unrelated settings — they now live in their own pane.

> 📍 Settings › Keyboard Shortcuts

— Exact navigation path given, mechanism is simple reorganisation

1Password for Windows beta 8.12.48-24 (… | 1Password for Mac beta 8.12.48-24 (2026…

1Password for Linux beta 8.12.48-24 (20…

04 **Exact-host login matching for non-standard ports** Not checked yet

IMPROVED

60

Logins saved on websites using a non-standard port (such as `nas.example.com:5001`) are now set to fill only on that exact host, preventing suggestions on other services on the same domain.

— Concrete example host given but no manual override shown

1Password in the browser 8.12.48-24 (20…

THINNER COVERAGE BELOW

05 **Steam Guard code support** Not checked yet NEW

50

1Password now saves Steam Guard codes in one-time password fields and displays Steam's five-character codes, on Android and in the browser extension.

Store a Steam account's rotating Guard code alongside the rest of your Steam credentials so 1Password surfaces the five-character code on demand.

> 📍 Open (or create) your Steam item › add a one-time password field › paste or scan your Steam Guard secret — 1Password will display the five-character code automatically.

— Behaviour described with an example, but no field/flag name

1Password in the browser 8.12.48-24 (20… 1Password for Android beta 8.12.48-24 (…

06 **Profile moved to account menu** Not checked yet IMPROVED

50

Profile has moved from the sidebar to the account menu, accessible by clicking your account name and choosing Profile.

— Exact navigation given, but it's a simple relocation

1Password for Linux beta 8.12.48-24 (20…

07 **Anti-Peek Mode removed** Not checked yet BREAKING

45

Anti-Peek Mode has been removed on Android and iOS; if it was enabled, Reveal Passwords and Allow Screenshots are no longer turned off by it and must now be managed independently.

— States the before/after but no migration steps given

1Password for iOS beta 8.12.48-24 (2026… 1Password for Android beta 8.12.48-24 (…

08 **DuckDuckGo support and browser re-approval fix on Windows**

Not checked yet NEW

45

1Password now works with DuckDuckGo on Windows, and browsers installed from the Microsoft Store or as app packages no longer require re-approval after each update.

— Names the browser and platform but no setup steps

1Password for Windows beta 8.12.48-24 (…

09 **Browser tab title shows vault context** Not checked yet IMPROVED

40

The browser tab title on 1Password.com now shows the current vault and list, and displays Editing when editing an item.

— Describes the change but gives no way to act on it

1Password for Mac beta 8.12.48-24 (2026…

10 **Compact edit button in Accounts & Vaults panel** Not checked yet

NEW

40

The Accounts & Vaults panel in the browser extension now has a compact edit button next to its title for choosing which accounts and vaults to show.

— Names the UI element but not exact navigation steps

1Password in the browser 8.12.48-24 (20…

11 **Credit card suggestions matched by title** Not checked yet IMPROVED

35

Credit card suggestions in the browser extension's inline menu now match on the card's title instead of its number.

— States the mechanism change but no way to configure it

1Password in the browser 8.12.48-24 (20…

12 **Website icons for API Credentials items** Not checked yet NEW

35

API Credentials that have a website now show the website's icon in the browser extension's item lists and search results.

— Clear visual change named but no interaction described

1Password in the browser 8.12.48-24 (20…

13 **Persistent notifications in Linux app** Not checked yet IMPROVED

30

Notifications, such as field-copy confirmations, now stay on screen until dismissed rather than auto-dismissing.

— Behaviour change stated with no navigation or control named

1Password for Linux beta 8.12.48-24 (20…

14 **Screen reader announces item section headings** Not checked yet

IMPROVED 30

Screen readers now announce section names as headings when viewing or editing an item.

— Accessibility change stated briefly with no further detail

1Password in the browser 8.12.48-24 (20…

UPDATED INTEGRATION HiBob custom field mapping

UPDATED INTEGRATION Rippling legal first name field mapping

UPDATED INTEGRATION UKG Ready rehire date import

NEW INTEGRATION Nice CXone SCIM URLs for external domains

└──▷ **BREAKING ON UPGRADE**

! Anti-Peek Mode has been removed; if it was enabled, Reveal Passwords and Allow Screenshots are no longer turned off by it and must be managed independently.

! Anti-Peek Mode has been removed. If it was enabled, it no longer keeps Reveal Passwords and Allow Screenshots turned off.

> 1Password SaaS Manager #2752 (2026-11-16) BLOG ↗ STABLE
>
> Adds five new AI spend columns, project-level consumption filtering on the main dashboard, and a per-user My AI consumption beta toggle in Settings > App catalog.
>
> Enable the My AI consumption beta for your organization in Settings > App catalog so individual users can see their own AI usage. Not checked yet
>
> Add five new columns to the spend explorer: Share of spend, Change against the previous period, Compared to average, Cost per request, and Cost per 1M tokens to compare cost across providers. Not checked yet
>
> Filter and report on external projects from the main consumption dashboard, not just from each app's Consumption tab, to see a project's AI usage across every app in one place. Not checked yet
>
> CSV exports from the spend explorer now use the same columns in the same order as the table. Not checked yet

WAS THIS USEFUL? 👍 👎

Auth0 Feedback ⓘ

OpenID Connect for Third-Party Apps is now Generally Available (2026-11-18)

BLOG ↗ RANK

Secure users, AI agents, and more with Auth0, a production-ready authentication and authorization platform built to help you ship faster and drive sign-ups.

> Auth0's headline release brings OpenID Connect for third-party apps to General Availability, adding per-app scope controls and Application Profile support for dynamically registered clients.

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

01 OpenID Connect GA for third-party apps Not checked yet NEW

75

Third-party apps can now be enabled for OIDC with control over which standard scopes (`profile` , `email` , `address` , `phone`) they may request, configured via OpenID Connect Settings in the dashboard (Applications > app > Settings > OpenID Connect Settings, Allow ID tokens). For apps created via dynamic registration with Client ID Metadata Documents, which cannot accept OIDC settings directly, OIDC is instead configured through Application Profiles so all apps registered under that profile inherit the setting. Enabled third-party apps now receive profile claims in the ID token, while the `/userinfo` endpoint returns only `sub` for those apps.

Turn on OIDC for a third-party app and restrict it to email and profile claims only.

> 📍 In the Auth0 dashboard, go to Applications › your third-party app › Settings › OpenID Connect Settings, enable Allow ID tokens , and check only `profile` and `email` under allowed scopes.

Enable OIDC for a dynamically registered app that cannot receive OIDC settings at registration time.

> 📍 In the Auth0 dashboard, go to Applications › Application Profiles › your profile › OpenID Connect Settings and enable OIDC there, so all apps registered via that Client ID Metadata Document inherit the setting.

— Exact dashboard paths and scope names given, but no API/CLI equivalent shown.

OpenID Connect for Third-Party Apps is …

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Omada Identity

Feedback ⓘ 18 November 2026 (2026-11-18)

BLOG ↗ RANK

Omada Identity is an identity governance and administration (IGA) platform that manages user access, enforces security policies, and automates lifecycle provisioning across enterprise systems.

> Omada Identity's SAP SuccessFactors connector gains two new authentication options to reduce dependency on external identity providers and an endpoint slated for deprecation.

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

01 **New authentication options for SAP SuccessFactors connector**

Not checked yet NEW 85

The SAP SuccessFactors connector now supports OAuth2 Client Credentials authentication via SAP Identity Authentication Service (IAS) using OpenID Connect (OIDC), selected via the Authentication type field in the collector or the Authentication mode parameter of the connector. It also supports OAuth2 SAML authentication without an external identity provider: leaving the SAML IDP Endpoint field empty causes Omada Identity to generate and sign the SAML assertion locally, avoiding a dependency on SAP's SAML assertion endpoint, which is scheduled for deprecation in May 2027.

Avoid a dependency on the SAP SuccessFactors SAML assertion endpoint (scheduled for deprecation in May 2027) by configuring local SAML signing — set Authentication mode to OAuth2 SAML and leave SAML IDP Endpoint empty in the connector settings.

> 📍 In the SAP SuccessFactors connector configuration, set Authentication mode to OAuth2 SAML and leave the SAML IDP Endpoint field empty. Omada Identity will generate and sign the SAML assertion locally.

— Names exact config fields, auth modes, and deprecation date.

18 November 2026 (2026-11-18)

WAS THIS USEFUL? 👍 👎

Ory

Feedback ⓘ

Ory Network, Ory Hydra, Ory Polis, Ory Elements v26.4.19 released NOTES ↗

RANK

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

> Ory added support for MCP clients and similar applications to sign in using client ID metadata documents, available on Enterprise plan projects.

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

01 **Client ID metadata document sign-in for MCP clients**

Not checked yet NEW 40

Ory Network now allows MCP clients and similar applications to sign in using client ID metadata documents. This capability is available on Enterprise plan projects.

– Names the capability and plan tier but no mechanism or setup steps

Ory Network, Ory Hydra, Ory Polis, Ory …

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Bedrock Security

Feedback ⓘ announced · Nov 18, 2026

PRESS ↗ RANK

Bedrock Security is a more than DSPM: Bedrock's AI and data security platform unifies data, identity, and AI context so teams see real risk — not noise — without moving data.

> Bedrock Security launched AI-assisted remediation that turns data exposure findings into Jira or ServiceNow tickets, verifies fixes, and can auto-revoke risky sharing through a policy engine — backed by natural-language routing overrides, in-ticket AI answers, and compliance-ready audit trails.

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

01 **Automated remediation tickets with fix verification**

Not checked yet NEW 70

A new AI-assisted remediation workflow automatically creates tickets in Jira or ServiceNow for each discovered data exposure, routes them to the identified data owner, and verifies the fix when the ticket is closed — reopening it if the exposure persists. Customers connect their existing Jira or ServiceNow instance to activate the workflow with no new tooling or training required for the teams making fixes.

— Mechanism and target tools named, but no API or config key given.

launch-20261118-3fd8d193

THINNER COVERAGE BELOW

02 **Natural-language routing rule overrides** Not checked yet NEW

50

Security teams can write natural-language routing rules to override default ticket assignment — for example, directing findings on a specific AWS account to one team unless the finding involves access permissions, in which case it routes to the identity and access team.

— Illustrative example given but no rule syntax or UI path. launch-20261118-3fd8d193

03 **Policy-based automatic revocation of sharing** Not checked yet

NEW 50

A policy engine can directly revoke document sharing based on sensitivity and other criteria without triggering a ticket workflow, notifying the data owner after the change is applied.

— Mechanism described but no policy config keys or console path. launch-20261118-3fd8d193

04 **Audit trail for remediation compliance** Not checked yet NEW

50

Every remediation ticket produces an audit trail with owner, timeline, and evidence of remediation to satisfy PCI DSS 4.0.1, SOC 2, and NYDFS Part 500 requirements.

— Names specific compliance standards but no export or report format.

launch-20261118-3fd8d193

05 **In-ticket AI answers for data owners** Not checked yet NEW

30

Bedrock Security's AI answers owner questions directly inside an open ticket — such as 'Who has access to this file?' — without requiring a separate investigation.

— Single example question, scope of Q&A unspecified. launch-20261118-3fd8d193

WAS THIS USEFUL?  

MIND

Feedback ⓘ

MIND and Microsoft: Better Together for the AI Era (2026-11-18) BLOG ↗ RANK

MIND data security platform puts data loss prevention (DLP) and insider risk management (IRM) on autopilot - automatically identify, detect & prevent data leaks

> MIND shipped a new Microsoft partnership integration covering Copilot prompt inspection, Graph-based file classification, unified DLP policy enforcement across files/Edge/Copilot, Entra ID identity context, and Exchange email DLP.

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

01 Unified DLP policy across files, Edge and Copilot

Not checked yet

NEW INTEGRATION NEW

65

A single DLP rule set now enforces across files, Microsoft Edge browser activity, and Copilot prompts on Windows 10 Build 1607 and later, with no minimum Edge version required.

– Gives concrete OS version threshold, still no exact config path

How MIND Integrates With Microsoft Copi…

02 Graph API classification of Copilot-reachable files

Not checked yet NEW INTEGRATION NEW

60

MIND's multi-layer classification engine classifies all files reachable by Copilot across SharePoint, OneDrive, and Teams attachments via the Microsoft Graph API, letting rollout teams see exposure before Copilot surfaces it.

– Names Graph API and three surfaces but no runnable step

How MIND Integrates With Microsoft Copi…

03 Entra ID identity context for policy decisions

Not checked yet

NEW

60

MIND pulls identity context from Microsoft Entra ID — groups, users, phone numbers, organizational trees, and activities — via the Graph API to drive policy decisions based on who can access sensitive data.

– Lists identity attributes pulled but no setup steps given

How MIND Integrates With Microsoft Copi…

THINNER COVERAGE BELOW

04 Real-time Copilot prompt inspection on Windows

Not checked yet

NEW SUPPORTED PLATFORM NEW

55

MIND's endpoint agent inspects Microsoft Copilot prompts in real time on Windows and blocks sensitive content before it leaves the device, covering both the browser-based and native Copilot app.

— Describes mechanism and scope but no config surface to act on

How MIND Integrates With Microsoft Copi…

05 **Exchange email DLP** Not checked yet NEW 40

MIND inspects Exchange email message bodies and attachments and blocks sensitive data from leaving the organization through email DLP.

— Thin one-line description with no mechanism detail

How MIND Integrates With Microsoft Copi…

NEW INTEGRATION Microsoft Information Protection SDK integration

NEW INTEGRATION Microsoft Exchange integration

MIND and Microsoft: Better Together for the AI Era (2026-11-18) BLOG ↗

LATEST STABLE

MIND signs a partnership agreement with Microsoft, extending DLP context and automation across the Microsoft environment.

MIND signs a partnership agreement with Microsoft to complement Purview labels with AI-driven discovery and contextual classification. Not checked yet

announced · Nov 18, 2026 PRESS ↗

MIND reaches general availability for its Microsoft 365 ecosystem integrations, now purchasable in the Microsoft Marketplace.

MIND is now available for purchase in the Microsoft Marketplace. Not checked yet

MIND's Windows endpoint agent now provides real-time data loss prevention across Copilot Desktop, Microsoft 365, and Edge applications. Not checked yet

WAS THIS USEFUL? 👍 👎

Clevis

Feedback ⓘ v25 CODE ↗ RANK

Clevis is a pluggable framework for automated decryption, enabling Linux systems to unlock encrypted volumes automatically using policies like TPM or Tang network servers.

> Clevis v25 trims the metadata it writes for Tang-bound volumes and adds display support for the Trustee pin type in LUKS configurations.

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

01 **Reduced LUKS header metadata for Tang bindings** Not checked yet

IMPROVED 78

Tang binding now calls `GET /version` at provisioning time and, when `tang_pub` is `true` in the response, stores only the Tang URL and key identifier in the JWE header instead of the full advertisement, reducing the metadata written to the LUKS header.

– Names exact endpoint and config flag but no runnable command. v25

THINNER COVERAGE BELOW

02 **Trustee pin shown in LUKS config display** Not checked yet NEW

45

LUKS config display now supports the `trustee` pin type, printing it alongside the existing `tang`, `tpm2`, and `null` pins.

– Clear addition but no mechanism or usage detail given. v25

WAS THIS USEFUL? 👍 👎

Cyera

Feedback ⓘ Cy Agents NOTES ↗ RANK

Cyera helps organizations protect data, govern identities, and secure AI agents to reduce risk, stay in control, and adopt AI with confidence.

> Cyera introduces Cy Agents, built-in AI agents that analyze sensitive data and context to surface exposure risks and prioritize alerts.

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

01 **Cy Agents for data exposure and DLP prioritization**

Not checked yet NEW 35

Cy Agents are specialized AI agents grounded in sensitive data, identities, access, activity, and business context. They uncover data exposure, prioritize DLP alerts, investigate activity, and answer plain-language questions.

— Describes purpose but no concrete UI path, config, or API detail. Cy Agents

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

amneziawg-installer

Feedback ⓘ v6.3.2 NOTES ↗ RANK

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

> This release of amneziawg-installer sharpens port diagnostics across `check`, `diagnose`, `port` and `--uninstall`, adds a `manage port` sync command, quiets a stale user-namespace warning on newer kernel modules, and updates the client compatibility table for the 3.1 profile.

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

01 manage port command to sync init port

Not checked yet NEW

90

Running `manage port <current port>` now writes the port into `awgsetup_cfg.init` and leaves all other configuration alone, letting admins sync a mismatched init port after a manual edit without a full reconfigure.

Bring `awgsetup_cfg.init` in line with the port currently in `awg0.conf` without touching any other configuration.

```
$ sudo bash /root/awg/manage_amneziawg.sh manage port <current port>
```

— Exact command given with a runnable example. v6.3.2

02 Richer port fields in check --json output

Not checked yet

IMPROVED

82

The port entry in `check --json` output now includes `source` and `init_mismatch` fields, showing whether the port came from `ListenPort` in `awg0.conf` or `AWG_PORT` in `awgsetup_cfg.init`, and whether the two disagree.

— Names exact JSON fields and config sources. v6.3.2

03 **Suppressed user-namespace warning on newer kernel module**

Not checked yet IMPROVED 80

`check` and `diagnose` now suppress the user-namespace warning when the loaded kernel module version is `3.1.20261113-02` or newer, reading the version from `/sys/module/amneziawg/version` for a loaded module or via `modinfo` for an unloaded one.

— Gives exact version threshold and lookup paths. v6.3.2

04 **Robust ListenPort parsing across commands** Not checked yet

IMPROVED 78

`check`, `diagnose`, `port` and `--uninstall` now parse `ListenPort` the way AmneziaWG applies it: stripping inline comments (`ListenPort = 51820 # ...`), using the last of multiple `ListenPort` lines, matching the key case-insensitively, and rejecting malformed values like `51820=x`.

— Lists exact parsing rules and affected commands. v6.3.2

05 **check/diagnose now read port from awg0.conf** Not checked yet

IMPROVED 76

`check` and `diagnose` now read the port from `ListenPort` in `awg0.conf` instead of `AWG_PORT` in `awgsetup_cfg.init`, so UFW-rule checks reflect the port the server is actually using after a manual config edit.

— Describes behaviour change but no new flag to invoke. v6.3.2

THINNER COVERAGE BELOW

06 **Client compatibility table updated for 3.1 profile**

Not checked yet IMPROVED 55

The client compatibility table was updated as of 16 November 2026, noting that Hiddify v5.9.8 pre-release reads `HeaderProtectionKey` and `ContentPaddingAddition` from the 3.1 profile, while stable v5.5.5 does not.

— Informational update with no action to take. v6.3.2

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

RegScale

Feedback ⓘ CLI 7.2.0 (2026-11-19) BLOG ↗ RANK

RegScale is a continuous compliance management platform that automates security documentation, assessments, and regulatory compliance workflows for organizations.

> RegScale's CLI 7.2.0 release adds a new `client_runs` command group for managing stuck sync runs and improves configuration load logging.

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

01 **client_runs subcommands for sync run management** Not checked yet

NEW 83

New CLI commands under `client_runs` let operators manage stuck synchronization runs: `regscale client_runs list` lists all sync runs left open by the current machine, `regscale client_runs status` inspects a single sync run, `regscale client_runs find` locates the sync run holding a specific plan and source, and `regscale client_runs close` closes a stuck sync run without cleanup.

— Names four exact runnable subcommands with their purposes. CLI 7.2.0 (2026-11-19)

THINNER COVERAGE BELOW

02 **Configuration source logging at INFO level** Not checked yet

IMPROVED 35

Every CLI command that loads configuration now logs at INFO level where its configuration came from and why.

— Describes behaviour but no exact log format or key named. CLI 7.2.0 (2026-11-19)

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI Runtime Defense & Guardrails

Operant AI

Feedback ⓘ

Your Customers Are Bringing Their Own Agents: Operant Personal Agent Defense Now Enables

NOTES ↗ RANK

Operant AI discovers, detects and defends AI applications, agents, MCP servers, APIs and Kubernetes workloads at runtime.

> Operant AI launched Personal Agent Defense, a verified edge built on the Poppy protocol that governs customer-side personal agents across conversation, MCP, API, and browser channels, adding admission control, per-tool entitlements, replay-safe approvals, OpenAPI-to-MCP compilation, and extending its semantic firewall, response scanning, and telemetry to cover them.

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

01 **Agent admission control and operation entitlements**

Not checked yet NEW 78

Teams can set per-agent stances of `trusted`, `blocked`, or `unknown` based on verified client ID rather than display name, so a lookalike agent cannot borrow a trusted agent's access. Operation entitlements let teams define per admitted agent which `MCP` tools and `OpenAPI` operations are allowed and which require a signed-in customer, specific scopes, task context, or explicit approval, with a missing or invalid policy defaulting to deny.

— Explains policy states, default-deny behaviour, and scoping mechanism

Your Customers Are Bringing Their Own A…

02 **OpenAPI-to-MCP compilation** Not checked yet NEW 78

OpenAPI-to-MCP compilation lets teams expose existing `OpenAPI` operations to personal agents as governed `MCP` tools over Streamable HTTP without rebuilding their stack; Operant compiles the operations and applies the same Poppy verification, task scope, response scanning, and approvals.

— Names transport and governance applied, but no exact command

Your Customers Are Bringing Their Own A…

03 **Validated poppy.json protocol declaration** Not checked yet NEW 70

Operant supplies a validated `poppy.json` document that teams publish on their own host to declare support for the Poppy protocol, with no changes required to OAuth servers, websites, or business APIs.

— Names the exact file and clear publish action a reader can take

Your Customers Are Bringing Their Own A…

04 **Replay-safe approvals via Poppy Operations v3** Not checked yet

NEW

65

Replay-safe approvals enforce Poppy Operations v3 for consequential actions — an approval is accepted only for the same owner, revision, and terms and executes at most once.

— Names the protocol version and exact replay-safety rule

Your Customers Are Bringing Their Own A…

05 **Per-session agentic telemetry for personal agents** Not checked yet

NEW

63

Per-session agentic telemetry records verified agent client ID, pseudonymous user ID, session, channel, conversation, tool or operation, message author, policy decision, task scope, approvals, and redactions across all channels.

— Lists every recorded field but no access path given

Your Customers Are Bringing Their Own A…

06 **Semantic Firewall extended to personal agents** Not checked yet

IMPROVED

60

The Semantic Firewall now covers personal agents: it stores the first message as the Session's task scope and evaluates every later message, tool call, and company-agent action across conversation, MCP, API, and browser channels against that scope.

— Describes mechanism but no config surface to act on

Your Customers Are Bringing Their Own A…

THINNER COVERAGE BELOW

07 **Response scanning and redaction for personal-agent traffic**

Not checked yet IMPROVED

51

Response scanning and redaction now covers personal-agent traffic, applying existing secret, prompt-injection, and hidden-text controls keyed on the agent's verified client ID.

— States scope of coverage but no new mechanism detail

Your Customers Are Bringing Their Own A…

08 **Personal Agent Defense verified edge** Not checked yet NEW

48

Operant adds Personal Agent Defense, a verified edge in front of conversation endpoints, MCP servers, OpenAPI operations, and joined browser sessions that

enforces identity, task scope, and approvals for personal agents built on the Poppy 1.0 protocol.

— Names the surfaces and protocol but stays at overview level

Your Customers Are Bringing Their Own A…

WAS THIS USEFUL? 👍 👎

◆ AI Security Posture & Discovery

Zenity Feedback ⓘ

Securing the Next Control Plane for AI Agents: Introducing Zenity for Sandboxes

NOTES ↗

Zenity discovers, secures and governs enterprise AI agents from buildtime to runtime across SaaS, endpoint and cloud.

Zenity adds a full sandbox security layer: discovery, posture checks with active red-team testing, runtime protection with taint and intent tracking, four containment levels, a trajectory view, and a new Sandboxes policy page.

A new Sandboxes page lets security teams write per-agent file, network, and runtime policies — including specific blocked paths, egress allow-lists, and environment variable listings by name — that the sandbox enforces directly. Not checked yet

New sandbox discovery continuously inventories every sandbox and sandbox template, linking each to its agent, credentials, workspace, egress policy, owner, image, and mid-session-installed packages, skills, and MCP servers, including shadow sandboxes and sandboxes without a managed platform. Not checked yet

Posture checks now flag misconfigured sandboxes — such as real API keys in the environment or image, wildcard egress rules, internet-reachable sandboxes, or root-running containers — as posture violations with risk descriptions and remediation guidance. Not checked yet

Posture is now also tested actively: a red-team agent runs inside each sandbox profile attempting to escape, reach denied hosts, read credentials, or tamper with hooks, and every path found becomes a hardening rule for that profile. Not checked yet

NEW DETECTION Runtime protection now evaluates each action against the full session context — combining harness intent, taint from untrusted content, and low-level process, file, and network telemetry — blocking actions that conflict with the agent's declared task. Not checked yet

+6 more

NEW INTEGRATION Sandbox platform integrations

NEW SUPPORTED PLATFORM Vendor-operated cloud coding agents

WAS THIS USEFUL? 👍 👎

Mend.io Mend AI

Feedback ⓘ (15-November-2026) NOTES ↗

RANK

Mend AI is a traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend AI added scan history tracking to monitor AI risk trends over time and improved scan reporting with violation counts and status visibility.

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

01 **Scan history and reporting improvements** Not checked yet NEW

37

Mend AI now surfaces scan history to track AI risk trends over time and compare findings across scans, and reports violation counts along with partial or failed scan statuses for more consistent reporting.

— Describes new reporting capabilities but no concrete UI path or API (15-November-2026)

WAS THIS USEFUL? 👍 👎

◆ AI Red Teaming & Testing

AI-Infra-Guard

Feedback ⓘ v4.6.11 NOTES ↗ RANK

AI-Infra-Guard is an open-source security scanning tool that detects vulnerabilities and misconfigurations in AI/ML infrastructure components like model servers and frameworks.

> AI-Infra-Guard's v4.6.11 release expands its detection rules for the one-api proxy and adds a new static operator to its Prompt-Security module for red-teaming chain-of-thought injection attacks.

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

01 **one-api fingerprint and vulnerability detection** Not checked yet

NEW 55

Adds a fingerprint rule for one-api to the fingerprints data set, and an authorization rule for `CVE-2026-81027` (channel-pinning in one-api) to the vulnerability rules data set.

— Names CVE and component but no scan command or scope shown. v4.6.11

02 **Static CoT-injection operator in Prompt-Security module**

Not checked yet NEW 45

Adds a single-turn static chain-of-thought (CoT) injection operator to the Prompt-Security module for red-teaming chain-of-thought injection attacks.

— Describes the operator's purpose but no usage details. v4.6.11

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

arsenal-ng

Feedback ⓘ v2.1 NOTES ↗ RANK

Arsenal-ng is the classic launcher, evolved. Fast, Go-based command library equipped with 250+ cybersecurity cheat-sheets.

> arsenal-ng v2.1 adds tab-completion for file paths when entering command arguments.

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

01 **Tab-completion for file path arguments** Not checked yet NEW

70

Argument input fields now support tab-completion for file paths: use Tab to cycle completions, or Ctrl+N / Ctrl+P to move through listed path suggestions.

— Names exact keys but no scope or limits given v2.1

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · November 19, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue