THE CYBER TOOLCHAIN

NO. 147

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED NOVEMBER 22, 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 71 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 16 tools

▾ // THE BRIEF

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

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. ScubaGear v2.0.0 collapses Defender, Purview, Exchange Online and Teams into one Security Suite baseline

vim ? help

with a config file that records why a policy was skipped. Snyk Code's `snyk fix --agentic` now chases vulnerabilities its own upgrades introduce. Minimal's Box Egress Proxy puts hash-chained audit records on what leaves a sandboxed box.

GOVERN

Assess an M365 tenant against one baseline and leave an auditor-readable record of every exception

ScubaGear's unified Security Suite baseline means one run covers Defender, Purview, Exchange Online and Teams instead of stitching separate reports, and the new configuration-file system lets you annotate, omit or exclude policies in a file that travels with the assessment — the compensating-control explanation stops living in a spreadsheet next to the output. Scrut adds a formal approval step and a status trend graph to risk items, so a risk's acceptance has a signatory and a history rather than a current state.

ScubaGear · Scrut Automation

PROTECT

Let the fixer finish the job instead of handing back an upgrade that opens something new

Dependency upgrades routinely introduce fresh advisories, and the usual loop is scan, fix, scan again, repeat by hand; `snyk fix --agentic` now follows that chain itself. Veracode's CLI recording DAST login sequences removes the Selenium IDE dependency that kept authenticated scan setup off the command line and out of CI.

Snyk Code · Veracode

DETECT

Keep a rule corpus from silently shadowing itself

Duplicate rule-name detection at collection-validation time catches the case where two Sigma rules share an identifier and one quietly wins — a failure that shows up as a detection that never fires rather than as an error. The configurable regex engine policy for SigmaMatcher makes matching behaviour explicit instead of dependent on whatever engine is installed.

pysigma

PROTECT

Record what a workload sent outbound, with evidence that holds up

> The Box Egress Proxy (`bep`) sits on the egress path with hash-chained audit records, leaf certificates, CA rotation and hardware-backed key storage, so the log of what a box talked to is tamper-evident rather than trusted on faith, and `min box audit` reads it back without exporting to a separate system.
>
> minimal

Does **Opus 5** read better? 👍 👎

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

xalgorix

Feedback ⓘ v4.6.202 NOTES ↗ RANK

> xalgorix v4.6.202 adds per-scan PID namespace isolation for process containment and fixes incorrect status notifications when resuming paused scans.

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

01 **Per-scan PID namespace isolation** Not checked yet NEW

91

Each scan now runs in its own PID namespace with its own `/proc`, so `ps`, `kill`, `pkill`, and `killall` run inside a scan can only reach that scan's own processes — the engine, other scans, and host services are unreachable. This can be disabled via the `XALGORIX_PROCESS_ISOLATION=false` environment variable or through the dashboard's Runtime settings panel.

— Names exact env var, UI path, and affected commands. v4.6.202

THINNER COVERAGE BELOW

02 **Fixed resume notification after engine restart** Not checked yet

IMPROVED

45

A resumed scan queue now sends a ' Scan Resumed' notification instead of a second ' Scan Started' message, including when resuming a previously paused scan.

— Describes the fix but no config or command to act on. v4.6.202

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Code Security

GitHub

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗ RANK

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

> GitHub's release centers on expanding Copilot across the stack — Evals, code review insights, customization source controls, new integrations, and CLI authentication via Microsoft Entra — alongside new on-demand secret scanning, bulk AI Scan, expanded OIDC audit log streaming, and a run of Copilot model/harness deprecations.

└──▷ **WHAT SHIPPED · 11 FEATURES** most completely described first ? what's the number?

01 **Copilot model and harness deprecations** Not checked yet DEPRECATED

65

GitHub is deprecating `MAI-Code-1.1-Flash` (removal in December), retiring the Local harness in VS Code (February 2027), and deprecated certain GitHub Copilot models as of November 16, 2026 — integrations using those model identifiers will stop working from that date.

— Names exact models, dates, and affected surfaces changelog-20261122-245ec4e7

02 **OIDC audit log streaming to S3 on GHE.com** Not checked yet

IMPROVED

60

Audit logs can now be streamed to Amazon S3 using OpenID Connect on GHE.com, expanding the existing OIDC-based streaming integration.

— Names target and auth mechanism, no config steps changelog-20261122-245ec4e7

THINNER COVERAGE BELOW

03 **`gh` CLI wait for pull request events** Not checked yet NEW

50

The `gh` CLI now supports waiting for pull request events, letting CI workflows block on a specific PR event instead of polling separately.

— Names the CLI capability but no flag syntax given changelog-20261122-245ec4e7

04 **On-demand secret scanning** Not checked yet NEW

50

Secret scanning can now be run on demand for developers and agents, without waiting for a push event to trigger it.

— Clear behaviour change, no trigger command named changelog-20261122-245ec4e7

05 **Microsoft Entra sign-in for Copilot CLI** Not checked yet NEW

50

GitHub Copilot CLI now supports signing in via Microsoft Entra as a preview authentication method.

– Names the exact auth provider, preview only changelog-20261122-245ec4e7

06 **GitHub Event Streams preview** Not checked yet NEW

50

GitHub Event Streams, in preview, lets consumers stream GitHub platform events for downstream processing.

– Names the feature and purpose, no endpoint or schema given changelog-20261122-245ec4e7

07 **Control over Copilot customization sources** Not checked yet NEW

50

Teams can now control which sources GitHub Copilot customizations come from, letting them restrict or pin customization origins.

– Describes control but no config key named changelog-20261122-245ec4e7

08 **Bulk AI Scan across repositories** Not checked yet IMPROVED

50

AI Scan can now be started in bulk across multiple repositories from a single action.

– Names the scale change, no UI path or command changelog-20261122-245ec4e7

09 **Copilot code review insights view** Not checked yet NEW

45

A new Repository insights view tracks GitHub Copilot code review outcomes.

– Names the UI surface but little mechanism detail changelog-20261122-245ec4e7

10 **New Copilot integrations: Supabase, Box, Calendly** Not checked yet

NEW

45

GitHub Copilot added new integrations with Supabase, Box, and Calendly.

– Names all three integrations, no setup detail changelog-20261122-245ec4e7

11 **GitHub Copilot Evals public preview** Not checked yet NEW

35

GitHub Copilot Evals, now in public preview, lets teams evaluate Copilot behaviour.

– Bare description, no methodology or metrics named changelog-20261122-245ec4e7

└──▷ **BREAKING ON UPGRADE**

! MAI-Code-1.1-Flash will be deprecated in December — workloads relying on that model must migrate before then.

! The Local harness in VS Code will be retired in February 2027.

! GitHub Copilot models deprecated on November 16, 2026 — any integrations using those model identifiers will stop working on that date.

WAS THIS USEFUL?  

Veracode

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗ RANK

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

> Veracode's CLI now records DAST login sequences without Selenium IDE, while DAST allowed URLs gain directory restrictions and Software Supply Chain Intelligence moves onto the unified REST API.

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

01 **DAST login recording via CLI** Not checked yet NEW 85

The new experimental `veracode dynamic record` command, shipped in Veracode CLI v2.56.0, records DAST login sequences in Chrome and saves them as a SIDE file for upload as a login script — no Selenium IDE installation required.

Record a login sequence for a web app so DAST can authenticate during a scan — without needing Selenium IDE installed.

```
$ veracode dynamic record
```

— Names exact command, version, and file format changelog-20261122-ab916929

THINNER COVERAGE BELOW

02 **Directory restrictions for DAST allowed URLs** Not checked yet NEW 40

You can now set directory restrictions when adding an allowed URL to a DAST web application target.

— Names the capability but no mechanism or UI path changelog-20261122-ab916929

03 **SSCI on unified REST API** Not checked yet IMPROVED 35

Software Supply Chain Intelligence (SSCI) now runs on the unified Veracode REST API.

— States the change with no detail on impact or endpoints changelog-20261122-ab916929

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Semgrep

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗ RANK

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

> Semgrep's latest release adds structured JSON scan logging, expands the hosted MCP server with job execution, team management and audit logging, and extends Supply Chain to flag unpinned Python dependencies, alongside editor and Managed Scans improvements.

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

01 JSON scan logs via SEMGREP_LOG_JSON_FILE

Not checked yet NEW

85

Setting the `SEMGREP_LOG_JSON_FILE` environment variable to a file path makes Semgrep write one JSON object per line for each phase start and finish, warning, and error, each tagged with the scan's details.

Pipe structured scan phase timings and errors into jq to diagnose why a large interfile scan timed out.

```
$ SEMGREP_LOG_JSON_FILE=/tmp/semgrep-scan.jsonl semgrep scan --config=auto . && jq 'select(.level=="warning")' /tmp/semgrep-scan.jsonl
```

Forward Semgrep's structured scan log to a log pipeline by writing JSON lines to a file and tailing it.

📍 `SEMGREP_LOG_JSON_FILE=/var/log/semgrep/scan.jsonl` semgrep scan `--config` =p/owasp-top-ten .

— Names exact env var and log structure, with runnable commands.

changelog-20261122-6af32516

02 Hosted MCP server job, team, project and audit capabilities

Not checked yet NEW

78

The hosted MCP server can run scan and workflow jobs from any MCP client via the `semgrep_run_job` tool, including clients that don't support MCP tasks. It can also list, create, update, and delete teams when your organization uses Teams to manage project access, and filter projects by tag and edit projects including their tags. Audit logs now record when an action was taken through the hosted MCP server, naming the MCP tool and client, and write an audit event for data-changing tool calls even when the underlying action previously did not.

– Names exact tool and actions but gives no UI path for each. changelog-20261122-6af32516

03 **Supply Chain findings for version-range dependencies**

Not checked yet NEW 75

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

– Names exact examples, label, and CLI version requirement. changelog-20261122-6af32516

04 **SSRF-scoped memories in Agentic Workflows** Not checked yet NEW 70

Write memories scoped to SSRF triage in Agentic Workflows by selecting `SSRF` under AI Detection in `Rules & Policies > Memories`.

– Exact UI navigation path given, but no further mechanism. changelog-20261122-6af32516

THINNER COVERAGE BELOW

05 **Open in editor links for Code findings** Not checked yet IMPROVED 55

Rule-based Semgrep Code findings now include an Open in editor link, and a finding's rule modal now includes Edit rule, both opening the rule in Semgrep Editor with the finding's file as test code scrolled to the finding's line.

– Describes behavior but names only UI labels, no paths. changelog-20261122-6af32516

06 **Paginated, filterable rule Library in Semgrep Editor**

Not checked yet IMPROVED 55

Semgrep Editor's Library now loads rules in pages and supports filtering by language, source, severity, visibility, and ownership, and grouping by folder or ruleset.

– Lists filter and grouping options but no exact navigation path.

changelog-20261122-6af32516

07 **GitLab Dedicated support in Managed Scans** Not checked yet NEW 50

GitLab Dedicated is now supported in Semgrep Managed Scans via the renamed GitLab Self-Managed or Dedicated option when connecting GitLab.

– Names exact option label but no further detail. changelog-20261122-6af32516

WAS THIS USEFUL?  

Snyk Code

Feedback ⓘ changelog · Nov 22, 2026 DOCS ↗

CHANGELOG ↗ RANK

Snyk Code is a static application security testing (SAST) tool that scans developer code in real time to identify and fix security vulnerabilities.

> Snyk Code's biggest addition this window is Snyk Studio, a new way to wire AI coding assistants into Snyk via an agentic installer and a local MCP server, alongside a more thorough `snyk fix --agentic` that now chases down vulnerabilities its own upgrades introduce.

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

01 Snyk Studio installation and management

Not checked yet NEW

90

Install Snyk Studio into AI coding assistants with `snyk studio install --experimental`, targeting specific assistants via `--ade=claude,cursor`, previewing changes with `--dry-run`, validating with `--verify`, and removing it with `--uninstall` or `--uninstall --dry-run`. Debug output can be inspected with `snyk studio logs --experimental --level=debug`. The installer also now places VS Code Copilot hooks in the correct location, adds MCP support for Antigravity, and lets you exclude a specific assistant from every install.

Bootstrap Snyk Studio for Claude and Cursor at the same time, then verify the installation succeeded — useful for onboarding a team where both assistants are in use.

```
$ snyk studio install --experimental --ade=claude,cursor --verify
```

— Names every flag and subcommand with a runnable example. 2026-11-22-a7b308dc

02 Agentic fix for self-introduced transitive vulnerabilities

Not checked yet IMPROVED

78

`snyk fix --agentic --auto-approve --issue-ids` now also remediates new vulnerabilities introduced by its own upgrades when they match `--severity-filter` or `--severity-threshold`.

Automatically fix vulnerabilities flagged in an Agentic Security Review report, including transitive issues introduced by the fixes themselves, without prompting for approval.

```
$ snyk fix --agentic --asr --asr-report ./asr-report.json --auto-approve --severity-filter=high
```

— Names flags and the before/after behaviour change precisely. 2026-11-22-a7b308dc

03 **Local MCP server in stdio mode** Not checked yet NEW 75

Run the local MCP server with `snyk mcp -t stdio`, or use a lighter profile via `snyk mcp -t stdio --profile=lite`, to give AI coding assistants direct access to Snyk tools.

Run the Snyk MCP server in lightweight mode for a local AI coding assistant that connects over stdio, reducing resource use on a developer machine.

```
$ snyk mcp -t stdio --profile=lite
```

— Exact command and flag given, but behaviour of 'lite' profile unexplained.

2026-11-22-a7b308dc

WAS THIS USEFUL? 👍 👎

Snyk Open Source

Feedback ⓘ changelog · Nov 22, 2026 DOCS ↗

CHANGELOG ↗ RANK

Snyk Open Source is a developer security tool that finds, prioritizes, and fixes vulnerabilities in open source dependencies within your projects.

> Snyk Open Source introduces Snyk Studio, an MCP-backed agentic scanning layer with its own install and diagnostics tooling, alongside a standalone local MCP server, new sbt 2 support, deeper pip dependency resolution, and a breaking change to npm vulnerability reporting accuracy.

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

01 Snyk Studio installation and diagnostics

Not checked yet NEW

85

Snyk Studio can be installed into AI-assisted development environments with `snyk studio install --experimental`, with optional flags `--ade=claude,cursor`, `--dry-run`, `--verify`, and `--uninstall` to customise or reverse the setup. Diagnostic output can be streamed at configurable verbosity with `snyk studio logs --experimental --level=debug`.

Bootstrap Snyk Studio into Claude and Cursor on a developer machine, then confirm what will change before committing.

```
$ snyk studio install --experimental --ade=claude,cursor --dry-run
```

Tail verbose Snyk Studio logs while troubleshooting an agentic scan that is not triggering.

```
$ snyk studio logs --experimental --level=debug
```

— Exact flags and commands given, but underlying mechanism of Studio itself unexplained

2026-11-22-54bda31e

02 Local MCP server for AI assistants

Not checked yet NEW

85

Snyk's local MCP server can run in stdio mode with `snyk mcp -t stdio`, or in a lighter footprint with `snyk mcp -t stdio --profile=lite`, and can be wired to any MCP-compatible assistant via `args: ['mcp', '-t', 'stdio']`.

Attach Snyk's MCP server to any stdio-compatible AI assistant so it can invoke Snyk tools directly during code generation.

```
$ snyk mcp -t stdio --profile=lite
```

– Exact command and config snippet provided for direct use `2026-11-22-54bda31e`

THINNER COVERAGE BELOW

03 **sbt 2 project scanning** Not checked yet NEW

55

Snyk Open Source now scans sbt 2 projects via `snyk test` and `snyk monitor`, requiring Java 17 or later.

– Names commands and Java requirement but no further mechanism `2026-11-22-54bda31e`

04 **Accurate npm peer dependency reporting** Not checked yet BREAKING

55

npm scans of projects with lockfile v2 or v3 may now show new vulnerabilities on upgrade, due to peer dependency and duplicate-package version reporting now being accurate.

– Explains cause and scope but no migration steps given `2026-11-22-54bda31e`

05 **Deeper pip dependency resolution** Not checked yet IMPROVED

45

pip scans now include packages pulled in through extras and respect environment markers on requirements.

– Describes what changed but no command or config to act on `2026-11-22-54bda31e`

└──▷ **BREAKING ON UPGRADE**

! npm scans of projects with lockfile v2 or v3 may show new vulnerabilities on upgrade, due to peer dependency and duplicate-package version reporting now being accurate.

WAS THIS USEFUL? 👍 👎

OpenQodex

Feedback ⓘ openqodex@0.22.1 NOTES ↗ RANK

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

> OpenQodex expanded `graph references` to catch more type-cast patterns across TypeScript, Python, and Go, improved floor caller-list reporting for test-only callers, and made killed-scanner errors and incomplete caller-list detection more precise.

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

01 **Cast-site coverage in graph references** Not checked yet IMPROVED

80

The `graph references` command now lists type usages in casts that were previously missed: TypeScript angle-bracket casts (`<Row>x`), import-type casts (`x as import('./types').Row`), Python typing.cast(Foo, x), cast('Foo', x), and cast(typ=Foo, val=x), and Go type assertions (v.(Bar)).

— Names every cast pattern and language it now covers openqodex@0.22.1

02 **Test-only caller detection in floor lists** Not checked yet IMPROVED

75

Floor caller lists now report `unknown.scope` as `tests` and set `unknown.note` to a sentence naming up to three hiding files when every potential hidden caller is in a test, fixture, corpus, benchmark, or top-level script, with the CLI printing that sentence after `floor:` .

— Names exact fields and output format but no example shown openqodex@0.22.1

THINNER COVERAGE BELOW

03 **Signal-aware scanner kill errors** Not checked yet IMPROVED

50

When a scanner is killed by a signal OpenQodex did not send, the error message now names the signal (for example, 'sqlfluff was killed by SIGKILL') instead of a generic sqlfluff was killed .

— Concrete example given but minor, no config surface openqodex@0.22.1

04 **Fewer false-positive floors in JS/TS caller lists** Not checked yet IMPROVED

50

Caller lists of TypeScript and JavaScript functions are now less often marked incomplete: a callback elsewhere in the package no longer marks every function's list a floor, and timers given a provable local function no longer keep a floor.

— Explains behavior change but lacks a concrete named surface `openqodex@0.22.1`

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

Cloudsmith

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗

RANK

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

> Cloudsmith made API key expiration rules generally available with independent schedules per account type, added CEP-16 sharded repodata support for Conda channels, and shipped CLI v1.31.0 with AI skills and build-tool credential helpers.

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

01 **Independent API key expiration rules per account type**

Not checked yet NEW 60

API key expiration and rotation rules are now generally available and can be set independently for user accounts and service accounts — for example, rotating user keys every 30 days while service account keys rotate every 60 days.

— Explains mechanism and gives concrete example but no exact config path

changelog-20261122-2e23f9be

THINNER COVERAGE BELOW

02 **CEP-16 sharded repodata for Conda channels** Not checked yet NEW

55

Conda channels now support `CEP-16` sharded repodata, letting compatible clients resolve dependencies without downloading an entire channel metadata file.

— Names the spec and benefit but no client setup steps changelog-20261122-2e23f9be

03 **CLI v1.31.0: AI skills and build-tool credential helpers**

Not checked yet IMPROVED 55

CLI v1.31.0 adds AI skills, and credential helpers for Maven, Gradle, and sbt, plus warnings for renamed CLI options.

— Names exact version and tools but no usage detail changelog-20261122-2e23f9be

WAS THIS USEFUL? 👍 👎

◆ Email Security

Abnormal AI

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗

RANK

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

> Abnormal AI's biggest release in this window adds interactive phishing coaching, three new AI agents for vendor, lateral, and mailbox-reported phishing, and a wave of new detectors spanning calendar invites, callback scams, prompt-injection text, coworker impersonation, and Microsoft 365/Entra ID identity threats.

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

01 **Microsoft 365 and Entra ID identity threat detections**

Not checked yet NEW 70

Adds compromised internal-sender detection from user phishing reports for Microsoft 365 (employee-reported phishing from a colleague's account feeds compromise detection even when the message itself scored safe), login-timing (time-of-week) anomaly detection that profiles each user's typical weekly login pattern and flags sign-ins outside normal hours, and low-and-slow brute-force detection for Identity Threat Protection customers that evaluates failed sign-in patterns across up to 7-day windows to catch paced credential-guessing campaigns.

— Specific mechanisms and windows named, no config exposed changelog-20261122-7cc9efbf

02 **New phishing detection models and signals** Not checked yet NEW

65

Adds a detector for phishing hidden inside calendar invite files, including fake invites that prior detection missed; a callback scam model that catches emails and attachments pushing recipients to call an attacker's phone number; new signals for punycode lookalike subdomains and invisible Unicode characters that may carry prompt-injection instructions; and a new detection layer for emails impersonating real coworkers such as fake file-sharing notifications and messages from lookalike personal email accounts. Also improves detection of phishing phrases and phone numbers disguised with invisible characters or look-alike digits.

— Names each detector but no manual trigger or config changelog-20261122-7cc9efbf

03 **Expanded attachment text and visual analysis** Not checked yet

IMPROVED 60

Expands attachment text detection to HTML, EML, calendar invites, and Office documents, and adds visual attachment analysis that scans QR codes and links inside attachments.

— Named formats but no user-facing control changelog-20261122-7cc9efbf

THINNER COVERAGE BELOW

04 **New AI Agents** Not checked yet NEW 55

Adds three new AI agents: a vendor AI agent for vendor email compromise that compares suspicious vendor emails against past correspondence and inspects links and attachments to automatically detect and remediate vendor email compromise, opening a vendor case on high-confidence verdicts; a lateral AI agent for internal phishing that reads email threads and weighs sender relationships and account takeover status to automatically triage and remediate internal phishing, opening an account takeover case on the sending account; and an AI agent classifier inside AI Security Mailbox that triages user-reported emails.

— Clear mechanism, no exposed config surface Clear mechanism, automatic trigger not user-invoked Names the product area but mechanism is thin

changelog-20261122-7cc9efbf

05 **Interactive Coaching in Just-in-Time Coaching pages**

Not checked yet NEW 50

Employees who click a risky email are walked back through it, review each red flag they missed, and retake a closing quiz with immediate feedback — the feature requires no setup.

— Mechanism described but no config or metric given changelog-20261122-7cc9efbf

06 **Spam bomb protection extended to low-volume attacks**

Not checked yet IMPROVED 40

Extends spam bomb protection to lower-volume attacks and to government customers, now remediating messages even when they resemble graymail.

— Scope of extension named, no mechanism detail changelog-20261122-7cc9efbf

07 **Expanded brand impersonation protection** Not checked yet IMPROVED 30

Expands brand impersonation protection to additional social media, collaboration, and AI brands commonly spoofed by attackers.

— No specific brands or numbers given changelog-20261122-7cc9efbf

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Snyk Container

Feedback ⓘ changelog · Nov 22, 2026

CHANGELOG ↗ RANK

Snyk Container scans container images and Dockerfiles for vulnerabilities, helping developers identify and fix security issues in their containerized applications.

> Snyk Container now reports image digests and can automatically reuse existing Docker credentials when testing or monitoring images.

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

01 **Automatic Docker credential fallback** Not checked yet IMPROVED

65

`snyk container test` and `snyk container monitor` can now be used without passing registry credentials explicitly — both commands fall back to your existing `docker login` credentials automatically.

— Clear command and behaviour change, directly usable 2026-11-22-c5b01e5e

THINNER COVERAGE BELOW

02 **Index and manifest digest reporting** Not checked yet NEW

55

`snyk container test` and `snyk container monitor` now include the index and manifest digests of an image reference in their output.

— Names exact commands and output addition, no deeper mechanism given 2026-11-22-c5b01e5e

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Huntress

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗ RANK

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

> Huntress shipped per-client overrides for RMM Guard, portal credential sign-in for its MCP integration, general availability of the redesigned Security Insights Report (replacing the legacy Threat Report), and a generally available ConnectWise Manage PSA Response Pod for in-ticket incident handling.

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

01 Per-client overrides in RMM Guard

Not checked yet NEW

90

Approve or reject an RMM tool for a single client organization without affecting the account-level decision for other clients. Use the Overridden filter in the RMM Tools Inventory to list all tools with organization-level decisions, and Reset to account default to remove an override; per-organization RMM Guard dashboards and tools inventory are now accessible under ESPM in the left navigation while viewing an organization.

Reject a specific RMM tool for one client without affecting other organizations — open that client's RMM Guard dashboard and act from the tool drawer.

> 📍 In the Huntress portal, navigate to the target organization › ESPM › RMM Guard. Open the tool drawer for the RMM tool and select Reject. To revert, choose Reset to account default.

Audit which RMM tools have organization-level overrides across your account to spot inconsistent decisions.

> 📍 In the Huntress portal, go to the account-level RMM Tools Inventory and apply the Overridden filter. Open any flagged tool to see each organization's decision and which ones show an Org override badge.

— Names exact filter, reset action and nav path with steps changelog-20261122-bd094142

02 Security Insights Report general availability

Not checked yet

85

BREAKING

Security Insights Report is now generally available for all accounts, replacing the legacy Threat Report, with monthly and quarterly views covering detection and response activity, security coverage, and SOC work; find it on the Reports page or receive it by

email to the same recipients as the legacy report. It adds two new EDR pages, Firewall Status Monitoring and External Recon, plus product-level breakdowns for Managed EDR, ITDR, SIEM, and ISPM and a cross-product Incident Summary page. Starting March 1, 2027, only the Security Insights Report will be generated and the legacy Threat Report will no longer be produced, so any workflow that forwards, parses, or archives the legacy report must be updated before that date.

— Names pages and deadline but only points to Reports page `changelog-20261122-bd094142`

---

03 **ConnectWise Response Pod for incident response** `Not checked yet`

NEW 80

ConnectWise Manage PSA Response Pod is now generally available, letting technicians approve or reject remediation plans, mark manual remediations complete, add comments, and resolve incident reports and escalations directly from a ConnectWise service ticket without switching to the Huntress portal.

Respond to a Huntress incident without leaving ConnectWise — approve remediation and resolve the escalation directly from the service ticket.

> 📍 In ConnectWise Manage (web or desktop), open the Huntress-generated service ticket. Use the Response Pod panel to review the remediation plan, select Approve, and then Resolve incident report once manual steps are complete.

— Gives in-ticket actions with example steps `changelog-20261122-bd094142`

└──▷ **BREAKING ON UPGRADE**

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

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

pysigma

Feedback ⓘ v2.1.1 NOTES ↗ RANK

pySigma is a Python library for parsing, transforming, and converting Sigma detection rules into backend-specific query languages for SIEM platforms.

> pySigma v2.1.1 adds duplicate rule-name detection during collection validation and introduces a configurable regex engine policy for SigmaMatcher.

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

01 Configurable regex engine via SigmaMatcher policy

Not checked yet

90

BREAKING

`SigmaMatcher` now accepts a `policy` argument to control which regex engine is used when compiling rule patterns, defaulting to the pipeline's policy. For example, passing SafePolicy() from `sigma.processing.conditions` enforces RE2 outside a full pipeline context. Under `SafePolicy`, rules using backreferences or lookaround now raise an error when the matcher is created.

Pass an explicit policy to SigmaMatcher to control the regex engine used when compiling rule patterns, for example to enforce RE2 outside of a full pipeline context.

```python
from sigma.matching import SigmaMatcher
from sigma.processing.conditions import SafePolicy

matcher = SigmaMatcher(rule, policy=SafePolicy())
```

– Names exact class, argument, policy, and breaking behaviour with runnable code v2.1.1

THINNER COVERAGE BELOW

02 Duplicate rule name detection in validation

Not checked yet NEW

35

Sigma rule collection validation now reports duplicate rule names, helping catch naming collisions across a rule set.

– States what changed but no mechanism or validation API shown v2.1.1

└──▷ **BREAKING ON UPGRADE**

! Under `SafePolicy`, rules that use backreferences or lookaround now raise an error when the matcher is created.

WAS THIS USEFUL?  

◆ SIEM

ClickHouse

Feedback ⓘ announced · Nov 19, 2026 BLOG ↗ RANK

ClickHouse is an open-source columnar database management system designed for real-time analytics and ultra-fast SQL queries on large datasets.

> ClickHouse shipped clickhousectl v0.6.0, adding Git-style project-root discovery, password-free Cloud authentication, a command search subcommand, shell completions, and Postgres 19 support, alongside pg_clickhouse 0.11.1, which adds pgvector type mapping with distance-operator pushdown and extends DML and aggregate pushdown to PostgreSQL.

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

01 **pgvector type mapping and distance-operator pushdown**

Not checked yet NEW 90

ClickHouse Array(Float32) and Array(Float64) columns can be mapped to PostgreSQL's `vector` type via `CREATE FOREIGN TABLE` with explicit column type definitions. pgvector distance operators `<->`, `<+>`, `<=>`, and `<#>`, plus equality `=` and `<>`, push down to ClickHouse's `L2Distance`, `L1Distance`, `cosineDistance`, and `dotProduct` respectively, and ClickHouse `vector_similarity` index usage (e.g. HNSW) is reported in EXPLAIN (VERBOSE) output via `Vector Index` and `Vector Index Not Used` plan lines.

Run nearest-neighbour vector search from PostgreSQL against a ClickHouse table backed by an HNSW index, using the pgvector L2 distance operator.

```
$ SELECT id FROM items ORDER BY v <-> '[0.3,-0.2,0.5,0.1]' LIMIT
5;
```

Map a ClickHouse Array(Float32) column to a PostgreSQL vector column so pgvector operators work over the foreign table.

```
$ CREATE EXTENSION vector;
CREATE FOREIGN TABLE items (
  id int NOT NULL,
  category text NOT NULL,
  v vector(4) NOT NULL
) SERVER ch_server;
```

— Names operators, functions, index type and includes examples. launch-20261119-a97d7b16

02 Project-root discovery and config merging for local commands

Not checked yet NEW 86

Running `clickhousectl local init` once marks a project root via `.clickhouse/`, and any local command run from a subdirectory walks up to find it the way Git walks up to `.git/`. The `CLICKHOUSECTL_PROJECT_DIR` environment variable pins a root for CI and monorepos, skipping directory-walk discovery, and server config is automatically merged from `~/.clickhouse/config.d/` (machine-wide) and `clickhouse/config.d/` in the project root before every `local clickhouse start`, so team config can be checked into the repo.

Initialise a project root so all local commands resolve correctly from any subdirectory, then start a named server and query it from a nested directory.

```
$ clickhousectl local init
clickhousectl local clickhouse start dev
cd src/app
clickhousectl local client dev --query "SELECT version()"
```

— Names env var, config paths, and includes a runnable example. launch-20261119-48fd8525

03 Password-free Cloud authentication and connection handling

Not checked yet NEW 86

`cloud clickhouse client` signs in through the browser as your Cloud user over native TLS without a password (requires ClickHouse 25.12+). `cloud clickhouse create --dotenv` writes a new service's connection settings and one-time password to a `.env` file instead of terminal output, and `cloud clickhouse dotenv <service-id>` retrieves an existing service's settings without a password, writing `CLICKHOUSE_HOST`, `CLICKHOUSE_PORT`, `CLICKHOUSE_HTTP_PORT`, `CLICKHOUSE_USER`, and `CLICKHOUSE_SECURE=true` to a file.

Create a new Cloud ClickHouse service and write its connection settings and one-time password to `.env.local` so the credential never appears in terminal output.

```
$ clickhousectl cloud clickhouse create --name analytics --ip-allow 203.0.113.10/32 --dotenv .env.local
```

— Exact flags, env var names written, and a runnable example. launch-20261119-48fd8525

04 Keyword search for CLI commands and flags Not checked yet NEW

72

A new top-level `search` subcommand finds any command or flag by keyword, with `--limit` (default 5) controlling result count and `--json` producing machine-readable

output.

Find which flags control IP access lists when you know the console term but not the CLI flag name.

```
$ clickhousectl search ip access list
```

— Flags and defaults named with a runnable example. launch-20261119-48fd8525

05 **Lightweight DML pushdown on MergeTree tables** Not checked yet

NEW 70

`UPDATE`, `DELETE`, and `TRUNCATE` statements on MergeTree family tables now push down as lightweight ClickHouse `UPDATE`, `DELETE`, and `TRUNCATE` statements.

Enable lightweight UPDATE support on a MergeTree table before issuing UPDATE statements through the foreign table.

```
$ CALL clickhouse_perform('ch_server', $$
  ALTER TABLE items
  MODIFY SETTING enable_block_number_column = 1,
enable_block_offset_column = 1;
$$);

UPDATE items SET v = '[1,1,1,1]' WHERE id = 0;
```

— Named statements with a runnable setup example. launch-20261119-a97d7b16

THINNER COVERAGE BELOW

06 **JSONB, timezone and numeric pushdown fixes** Not checked yet

IMPROVED 55

JSONB subscript syntax `data['a']['b']` now pushes down to ClickHouse column dot notation. On ClickHouse 23.6+, `session_timezone` is always set to match the PostgreSQL `TimeZone` and passed to `DateTime` functions. Bare `NUMERIC` columns now use Decimal(76, 38), the largest possible ClickHouse decimal size, with trailing zeros trimmed from results.

— Three concrete type/pushdown fixes named, no examples given. launch-20261119-a97d7b16

07 **NULL-returning aggregate pushdown** Not checked yet IMPROVED 50

Aggregate functions like `sum`, `avg`, and `min` now push down as `sumOrNull`, `avgOrNull`, and `minOrNull`, returning NULL instead of a ClickHouse default value (e.g. 0) when aggregating no values.

– Clear before/after behaviour but no runnable example. launch-20261119-a97d7b16

---

08 **Shell completions and feedback subcommand** Not checked yet NEW

45

`clickhousectl completions <shell>` enables Tab completion for `clickhousectl` and `chctl` in bash, zsh, or fish when added to a shell startup file. A new `feedback` subcommand sends free-text feedback, up to 500 characters, directly to the ClickHouse team.

– Commands named but no example or deeper mechanism given. launch-20261119-48fd8525

---

09 **Postgres 19 support in Managed Postgres** Not checked yet NEW

40

Services can now be created on ClickHouse Managed Postgres running Postgres 19 using `postgres create --pg-version 19`.

– Single flag named, no further detail given. launch-20261119-48fd8525

---

10 **OAuth re-login required after v0.6.0 upgrade** Not checked yet

30

BREAKING

OAuth logins saved by clickhousectl v0.5.x require one fresh login after upgrading to v0.6.0.

– States the break but gives no migration steps. launch-20261119-48fd8525

NEW INTEGRATION ClickHouse Arrow Flight SQL connector for Power BI (public preview)

└──▷ BREAKING ON UPGRADE

! OAuth logins saved by v0.5.x require one fresh login after upgrading to v0.6.0.

> announced · Nov 19, 2026 BLOG ↗
>
> ClickHouse adds an Arrow Flight SQL connector for Power BI in public preview, enabling direct columnar transfer via gRPC/TLS with no gateway, query folding, and faithful Decimal/UInt64 types.
>
> Enable the Arrow Flight interface on self-managed ClickHouse (26.5 or later) via `<arrowflight_port>`, `<enable_ssl>`, `<ssl_cert_file>`, and `<ssl_key_file>` in `clickhouse` config to expose a gRPC/TLS endpoint on port `9090`.
>
> Not checked yet
>
> ClickHouse adds an Arrow Flight SQL connector for Power BI, now in public preview, that connects Power BI directly to ClickHouse over Arrow Flight SQL with no on-premises data gateway required. Not checked yet

> Query folding pushes filters, sorts, group-bys, and inner joins from Power Query down to ClickHouse as SQL, so only needed results are returned. Not checked yet
>
> Pass arbitrary SQL directly through Power Query using `Value.NativeQuery` for full control over what ClickHouse executes. Not checked yet
>
> Decimal and UInt64 column values now reach Power Query without floating-point conversion. Not checked yet
>
> +1 more

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

JumpCloud

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗

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 adds separate DDM enforcement settings for major and minor macOS updates, and a consolidated Restrictions policy for macOS and iOS/iPadOS under Device Management > Policy Management.

UPDATED SUPPORTED PLATFORM Configure enforcement for major macOS upgrades and minor macOS updates independently in the declarative device management (DDM) Automatic macOS Updates policy, with separate grace periods and local enforcement times for each update type. Not checked yet

NEW SUPPORTED PLATFORM Manage Apple device restrictions for macOS and iOS/iPadOS through a single Restrictions policy under Device Management > Policy Management, covering system settings, privacy and security, biometrics, iCloud, and Apple Intelligence & Siri. Not checked yet

NEW INTEGRATION New macOS and Windows apps added to JumpCloud App Catalog

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Compliance Automation & Trust Management

Compyl

Feedback ⓘ changelog · Nov 22, 2026 CHANGELOG ↗

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

Compyl adds custom fields on Questionnaires and Controls, bulk blueprint scheduling, Trust Center access-request workflows, and Google Drive policy publishing.

Add custom fields to Questionnaires: admins can create an extension form, and the fields appear on each questionnaire and can be queried in Query Builder.
Not checked yet

Add custom fields to Controls: admins can define them, users can view and edit them in the control drawer, see them as columns in the Controls grid, and fill them in through CSV import. Not checked yet

Set a bulk run schedule for blueprints to move many blueprints to a new cadence (for example, monthly to daily) in one step. Not checked yet

Trust Center Admin module now lives at `/trust-center-admin` in the navigation, breadcrumb, and page title, freeing up `/trust-center` for the public Trust Center page. Not checked yet

Trust Center access requests now reach reviewers: requests go straight to Pending, reviewers are emailed on arrival, and visitors are notified when a decision is made.
Not checked yet

+3 more

NEW INTEGRATION Microsoft Sentinel sync

NEW INTEGRATION Duo managed endpoint sync

NEW INTEGRATION Azure SQL Server firewall rules sync

NEW INTEGRATION Azure storage account settings collection

WAS THIS USEFUL? 👍 👎

GOVERN

◆ Model & Agent Protection

Minimal Software Research minimal

Feedback ⓘ

release-97724242 NOTES ↗ RANK

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

> Minimal shipped a Box Egress Proxy (`bep`) with hash-chained audit records, leaf certificates, CA rotation and hardware-backed key storage, alongside new `min secret` and `min box audit` commands, opt-in OpenTelemetry tracing across its binaries, and a breaking removal of the old `min stop` and `min task run --path` verbs.

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

01 **Box Egress Proxy (bep) with hardware-backed keys** Not checked yet

NEW 93

Adds the Box Egress Proxy (`bep`) with hash-chained audit records, leaf certificates issued under a name-constrained root, CA rotation through a control socket, and store-rule enforcement. `bep serve` takes `--max-client-keys` to bind client keys, store rules live under `min --config-dir` in step with `bep serve` , and proxy keys are held in the host keychain, Secure Enclave (macOS), TPM (Linux), or Secret Service (Linux, when no usable TPM) depending on platform. A signed, notarized `bep` binary ships beside `minvmd` on macOS and starts alongside `gvproxy` so `git` and `gh` reach GitHub from inside a VM, proxying runtime-published ports like a direct connection.

— Full mechanism and flags named, but no direct runnable bep example release-97724242

release-7ff9a855

02 **Structured output and network view for box show** Not checked yet

IMPROVED 70

`min box show <box> -o json` or `-o yaml` returns a box's current spec, including its declared execs, for programmatic inspection, and `min box show <box> --network` shows the box's network effect to verify egress policy before running an agent.

Export a box's current spec as JSON for programmatic inspection of its declared execs and store references

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

Inspect a box's declared network effect to verify egress policy before running an agent.

```
$ min box show mybox --network
```

— Two runnable commands with exact flags and output formats release-7ff9a855 release-97724242

03 **Box audit trail command** Not checked yet NEW 65

`min box audit <box> --parent` inspects a box's full audit trail, merging in its parent box's records, to review every proxy decision after a suspected policy violation.

Inspect a box's full audit trail, merging in its parent box's records, to review every proxy decision

```
$ min box audit mybox --parent
```

Audit a box's egress history and merge its parent chain in one view — useful after a suspected policy violation.

```
$ min box audit --parent mybox
```

— Clear purpose with exact runnable command release-7ff9a855 release-97724242

04 **Removal of old session verbs** Not checked yet BREAKING 65

The old session verbs `min stop` and `min task run --path` are removed; use `min host stop` and `-C <dir>` instead.

— Exact before/after commands given for migration release-97724242 release-7ff9a855

THINNER COVERAGE BELOW

05 **min secret for runtime credentials** Not checked yet NEW 55

`min secret set MY_API_TOKEN` stores a secret token for a box so it is available at runtime without pasting credentials into the session.

Store a secret token for a box so it is available at runtime without pasting credentials into the session.

```
$ min secret set MY_API_TOKEN
```

— Runnable command given, little on storage mechanism release-7ff9a855

06 **Opt-in OpenTelemetry export** Not checked yet NEW 50

Adds opt-in OpenTelemetry export with a local spool across the CLI (`min`), daemon (`minimald`), and VM host daemon (`minvmd`).

— Names the three binaries but no enabling flag or config key release-97724242

07 **Cleaner non-terminal box logs** Not checked yet IMPROVED 30

Strips terminal control codes in `min box logs` when stdout is not a terminal.

— Small, clearly scoped fix with exact command named release-97724242

08 **Detach keys for exec attach** Not checked yet IMPROVED 20

Detaching from an exec attach now uses configured detach keys.

— No specifics on key configuration or defaults release-7ff9a855

09 **QUIC block helper naming in finalize-install** Not checked yet IMPROVED 20

Names the QUIC block helper in `min finalize-install` .

— One-line change with little mechanism explained release-97724242

└──▷ **BREAKING ON UPGRADE**

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

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

WAS THIS USEFUL?  

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · November 22, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue