THE CYBER TOOLCHAIN

NO. 072

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 12, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 170 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 31 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. ConductorOne's Agent Classifiers judge an AI agent's call as it happens and can block it or force a human

vim ? help

approval, not just log it after. TruffleHog's `--verifier` flag points secret verification at your own enterprise endpoints instead of the vendor's. Elastic Security Labs shipped Linux privilege-escalation rules covering SUID/SGID abuse and page-cache kernel bugs.

GOVERN

Stop a rogue AI agent call mid-flight instead of reading about it afterwards

ConductorOne evaluates agent risk at call time with block, human-approval routing, or an Observe mode you can run first to see what would have fired. JumpCloud's Agent Identities give non-human agents a real identity to attach policy to, and AppOmni adds an Agent Inventory so you at least know which agents exist in your SaaS estate before writing rules for them.

ConductorOne · JumpCloud · AppOmni

DETECT

Catch Linux local privilege escalation with rules that already map to ATT&CK

Elastic's layered framework pairs SIEM and endpoint rules for SUID/SGID abuse and page-cache/COW kernel bugs with Auditd Manager guidance, so teams get a working starting point on a detection surface most SOCs cover thinly. Velociraptor's new ADCS ESE parser gives responders a way to pull certificate-authority database artifacts during a hunt, where ADCS abuse is now a standard escalation path to domain admin.

Elastic Security Labs · Velociraptor

PROTECT

Verify secrets against your own endpoints, and cut the CVEs your code never calls

TruffleHog's `--verifier` flag and `customVerifiers` config let self-hosted GitHub, GitLab or Artifactory installs be checked for live credentials rather than being written off as unverifiable, and `--sarif` drops the results straight into GitHub Code Scanning. Socket's reachability engine now covers PHP/Composer and monorepo workspaces and can be pinned to a version, so a CI gate does not shift verdicts under you; Veracode's LA CLI command auto-remediates SCA findings rather than filing them.

trufflehog

Does **Opus 5** read better? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

ZeroPath

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

ZeroPath is an AI-native SAST platform that finds 2x more real vulnerabilities with 75% fewer false positives.

> ZeroPath's biggest window addition is a hosted remote MCP server for AI coding assistants, paired with a new Continuous Scanning mode that rescans on every commit to a default branch and new Gerrit and CVS source-control integrations; the release also adds Microsoft Teams alerts, Assistant skills, and several breaking changes to scan-failure fields, integration permissions, and finding review status.

└──▷ WHAT SHIPPED · 20 FEATURES most completely described first ? what's the number?

01 **Continuous Scanning mode for default branches** NEW

79

Continuous Scanning triggers a full scan on every meaningful commit to a default branch, including merged pull requests, with follow-up scans closing findings fixed by those commits. It's configurable per organization, tag, or repository on GitHub, GitLab, Bitbucket Cloud, and Bitbucket Server.

— Explains trigger, scope and configurable levels changelog-20260912-ed06a3ad

02 **`lastScanFailure` field replaces `lastScanError`** BREAKING

73

Repository objects now expose `lastScanFailure`, replacing `lastScanError`, carrying both the error message and the outcome. Any integration or script reading `lastScanError` will receive no value after upgrade.

— Names exact field change and breakage impact changelog-20260912-ed06a3ad

03 **Pull request submission status tracking** NEW 73

Approved patches now show pull request submission status — queued, in-progress step, retry state, or stop reason — with Cancel and Retry actions and up to five automatic submission attempts. A completed pull request scan links to the findings list it produced, with a separate dependency findings link.

— Names states, actions and attempt limit changelog-20260912-ed06a3ad

04 **CVS integration for full and dependency scans** NEW

70

ZeroPath imports CVS modules by server path over SSH or pserver for full scans, scheduled scans, dependency analysis, and secrets scanning.

— Names protocols and scan types supported `changelog-20260912-ed06a3ad`

05 **Jira and Linear ticketing enhancements** NEW 70

CSV exports and the export endpoint now include Jira and Linear ticket links. An on-demand Jira ticket sync preview shows each linked ticket's pending action before you apply it. Ticket creation for Jira and Linear is now a per-repository permission requiring an explicit grant when access control is enabled.

— Names export surfaces, preview feature and permission gating `changelog-20260912-ed06a3ad`

06 **Gerrit integration for full and patch-set scans** NEW 68

ZeroPath imports Gerrit projects for full scans and scans each open change as new patch sets arrive, posting findings as a review message on the patch set.

— Describes import, patch-set scanning and review posting `changelog-20260912-ed06a3ad`

07 **Assistant skills for reusable methodologies** NEW 68

Assistant skills are reusable methodology definitions — triage, dependency reachability, report writing, patch review — that the Assistant applies while working. They're authorable from the Skills tab, with four built-in forkable skills.

— Names skill types and UI location for authoring `changelog-20260912-ed06a3ad`

08 **Unassessed findings now surface as 'Needs Review'** BREAKING 65

A finding ZeroPath has not assessed now appears in the queue as Needs Review, ranked on severity alone — widening the previous rule that only verified findings appeared, so open counts will rise after upgrade.

— Explains behavior change and its impact on counts `changelog-20260912-ed06a3ad`

THINNER COVERAGE BELOW

09 **Wiz export resolves and syncs dependency findings** NEW 59

On first export, ZeroPath marks already-resolved dependency findings as resolved in Wiz and sends unassessed findings as new records.

— Explains exact export behavior and mechanism `changelog-20260912-ed06a3ad`

10 **More languages counted in repository size** IMPROVED

58

Terraform, Svelte, Vue, Solidity, Elixir, Dart, protobuf, and Genero are now included in repository size calculations, qualifying those repositories for deeper analysis.

– Lists all eight languages added changelog-20260912-ed06a3ad

11 **Dependency findings tab on Issues page** NEW

57

A new dependency findings tab on the Issues page supports CVE, advisory, and package search.

– UI path and search fields named, no deeper mechanism changelog-20260912-ed06a3ad

12 **Scoped tag and repository filtering in reports** IMPROVED

57

Monthly, organization summary, SLA compliance, and SOC 2 reports now support scoped tag and repository filtering, stated on the report cover.

– Names all four report types affected changelog-20260912-ed06a3ad

13 **Scope control in Supply Chain view** NEW

55

A scope control at the top of Supply Chain narrows all tabs to a selected set of repositories, teams, and tags.

– UI location and filter dimensions named changelog-20260912-ed06a3ad

14 **Secret dismissal explanations withheld from API** BREAKING

54

For secret findings, the explanation ZeroPath generates for a dismissal is now withheld from API responses; only a reviewer's own note is returned.

– Names exact API behavior change changelog-20260912-ed06a3ad

15 **Severity labels aligned to CVSS bands** IMPROVED

53

Severity labels now follow CVSS rating bands: Critical ≥ 9.0, High ≥ 7.0, Medium ≥ 4.0, Low ≥ 0.1.

– Exact numeric thresholds given changelog-20260912-ed06a3ad

16 **CVSS v4.0 vector support** NEW

50

ZeroPath now supports CVSS v4.0 vectors, assessing subsequent-system impact on its own evidence.

– Names version and unique assessment detail changelog-20260912-ed06a3ad

17 **Secrets scanning coverage reporting** IMPROVED

50

Secrets scanning now reports the coverage it achieved, naming any file too large to read within the scan's time budget.

— Names time-budget constraint mechanism `changelog-20260912-ed06a3ad`

---

18 **'What's new' release panel** NEW 40

A What's new panel in the top bar surfaces the three most recent releases, with unread indicators.

— Thin UI-only description `changelog-20260912-ed06a3ad`

---

19 **Dashboard full-year and quarterly views** IMPROVED 40

The dashboard now covers a full year at a glance, with a quarterly period option.

— Thin UI-only description `changelog-20260912-ed06a3ad`

---

20 **GitHub Enterprise Cloud with data residency support** NEW 30

GitHub Enterprise Cloud with data residency is now a supported version control host.

— Thin one-line addition, no mechanism given `changelog-20260912-ed06a3ad`

└──▷ BREAKING ON UPGRADE

! On repository objects, `lastScanError` is replaced by `lastScanFailure`; any integration or script reading `lastScanError` will receive no value after upgrade.

! On secret findings, the explanation ZeroPath generates for a dismissal is withheld from API responses; only a reviewer's own note is returned.

! Connecting an integration now requires the Create Integrations or Create Installations permission; adding a repository by URL requires Create Repositories.

! A finding ZeroPath has not assessed now appears in the queue as Needs Review (ranked on severity alone), widening the previous rule that only verified findings appeared — open counts will rise after upgrade.

WAS THIS USEFUL? 👍 👎

GitHub

Feedback ⓘ 3 RELEASES · 2026-09-10 → 2026-09-11 BLOG ↗ RANK

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.

> GitHub's biggest ships this window were on Copilot: a new adaptive model router (HydraFusion) in Copilot CLI, expanded VS Code agent capabilities (automations, voice mode, in-window PR review), a Jira integration in the Copilot app, JetBrains enterprise sandbox controls, deeper Copilot code review analysis, and new VS Code Agents fields in the Copilot usage metrics API.

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

01 HydraFusion adaptive model routing in Copilot CLI NEW

83

`Project HydraFusion` is now available under `/experimental` in Copilot CLI, providing automated semantic routing between local, cloud, and compound models. Select it like any other model and it balances performance, cost, and latency per task.

Route a high-latency coding task through the best available model automatically, instead of manually choosing between local and cloud models.

> 📍 In Copilot CLI, open the model selector and choose `HydraFusion` (listed under `/experimental`) — submit your task as normal and HydraFusion selects the local, cloud, or compound workflow based on cost and latency.

— Names the model, menu location, and gives a runnable usage example

GitHub Copilot weekly releases — Septem…

02 VS Code Agents fields in Copilot usage metrics API IMPROVED

73

The Copilot usage metrics API adds VS Code Agents fields: `daily_active_vscode_agent_users` (unique users active in the VS Code Agents window per 1-day/28-day period) and `totals_by_vscode_agent` (optional `session_count` and `total_user_messages` rollups) in aggregate enterprise/organization reports, plus `used_vscode_agent` and per-user `totals_by_vscode_agent` in per-user reports.

— Names every field added but not the endpoint path itself

Add VS Code Agents to Copilot usage met…

03 Centralized sandbox policy controls for JetBrains NEW

71

Public preview of centralized sandbox policy controls for GitHub Copilot in JetBrains IDEs, letting enterprise administrators govern sandbox enablement, filesystem and network access, proxy settings, developer-tool access, and macOS Keychain access.

— Names every governed control area but not the admin console path

GitHub Copilot weekly releases — Septem…

THINNER COVERAGE BELOW

04 **Smart commit messages and shell-tool analysis in code review**

IMPROVED

50

Copilot code review now generates smart commit messages when you apply an autofix suggestion, describing the specific change instead of a generic message, and expands its analysis to use the full set of shell tools from the Copilot SDK — including running build commands, tests, and targeted scripts — behind the Copilot agent firewall.

▶ Watch video

— Explains mechanism but gives no flag or command to invoke it

Auto-resolution and analysis updates in…

05 **Jira integration in Copilot app canvas** NEW

45

Copilot app adds a Jira integration that lets you bring Jira issues into a shared canvas and carry context through investigation, implementation, and pull request preparation.

— Describes the flow but no exact commands or config

GitHub Copilot weekly releases — Septem…

06 **Agent automations in VS Code** NEW

43

Public preview of agent automations in VS Code 1.137, enabling recurring agent tasks scheduled hourly, daily, or weekly, or triggered on demand.

— Explains scheduling options but no config or command

GitHub Copilot weekly releases — Septem…

07 **Issue and PR review in Agents window** NEW

42

VS Code 1.137 (experimental) adds the ability to review issue and pull request details directly in the Agents window, even when the repository is not open.

— Names the UI surface and a concrete before/after condition

GitHub Copilot weekly releases — Septem…

08 **Voice mode for Copilot in VS Code** NEW

33

Experimental voice mode in VS Code 1.137 allows you to talk to, interrupt, or redirect Copilot while it works on your code.

— Describes interaction but no activation steps GitHub Copilot weekly releases — Septem…

WAS THIS USEFUL?

Cloudsmith

Feedback

1 RELEASE · 2026-09-11 BLOG ↗ RANK

A fully-managed, enterprise-scale solution to control, secure, and distribute software packages and containers.

> Cloudsmith improved GitHub secret scanning alerts to pinpoint exactly where an exposed API key was found.

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

01 Direct links in secret scanning notifications IMPROVED

50

GitHub secret scanning email notifications now list every detection location for an exposed Cloudsmith API key, with a direct link to each occurrence in the GitHub repository.

— Explains the change but no config or command surface given

GitHub secret scanning notifications no…

WAS THIS USEFUL?

Black Duck

Feedback ⓘ 1 RELEASE · 2026-09-10 BLOG ↗ RANK

Black Duck helps organizations secure their software supply chain by providing deep visibility into open source components, licenses, and vulnerabilities.

> Black Duck Signal adds bring-your-own-LLM support, letting each of its seven AppSec agents be routed through customer-controlled LLM infrastructure instead of Black Duck-managed endpoints, plus a preflight check to validate those endpoints before a scan runs.

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

01 **BYO-LLM support with per-agent model routing** NEW 95

Adds a `--llm-mode` CLI flag and `mode` field in the `[LLM]` config-file section to switch Black Duck Signal between Black Duck-managed and BYO-LLM endpoints. The global `[LLM]` section sets `uri`, `key`, `timeout`, `gcp_service_account_key`, and `gcp_project` defaults for all seven agents, while per-agent sections — `[LLM_SINGLEFILESCAN_AGENT]`, `[LLM_DATAFLOW_AGENT]`, `[LLM_OVERSIGHT_AGENT]`, `[LLM_EXPLOITATION_AGENT]`, `[LLM_SCA_AGENT]`, `[LLM_MERGEKEY_EMBED_AGENT]`, `[LLM_OVERSIGHT_EMBED_AGENT]` — accept `model`, `uri`, `key`, `timeout`, and `api_version` overrides so each agent (single-file SAST, cross-file dataflow, oversight, exploitation, SCA, and two embedding agents) can target a different provider, model, and endpoint within one scan. Supported BYO-LLM providers are OpenAI direct API, Azure OpenAI (including Azure AI Services with native Anthropic Claude and automatic Claude-vs-OpenAI family detection), AWS Bedrock via IAM bearer-token auth, GCP Vertex AI with native service-account credentials and automatic token refresh, and any OpenAI-compatible proxy including LiteLLM.

Route the high-volume single-file SAST agent to a cost-optimised model while keeping lighter agents on a cheaper model, all within your own Azure OpenAI tenancy.

```ini
[LLM]
mode = byo
uri = https://your-endpoint.example.com/v1
key = ${OPENAI_API_KEY}
timeout = 600

[LLM_SINGLEFILESCAN_AGENT]
model = gpt-4o
timeout = 600

[LLM_DATAFLOW_AGENT]
model = gpt-4o-mini

[LLM_OVERSIGHT_AGENT]
model = gpt-4o-mini

[LLM_EXPLOITATION_AGENT]
model = gpt-4o-mini

[LLM_SCA_AGENT]
model = gpt-4o-mini

[LLM_MERGEKEY_EMBED_AGENT]
model = text-embedding-3-large

[LLM_OVERSIGHT_EMBED_AGENT]
model = text-embedding-3-small
```

Use GCP Vertex AI for all agents to satisfy data-residency requirements, supplying a service-account key and project so Signal handles token refresh automatically.

```ini
[LLM]
mode = byo
gcp_service_account_key = gcp-sa-key.json
gcp_project = your-gcp-project-id
```

— Every config key, section and provider named with runnable config examples

Agentic AppSec on your infrastructure w…

02 **LLM endpoint preflight validation** NEW 60

Adds a `--check-llm` preflight flag that validates every configured LLM endpoint is reachable and authenticated before a scan runs, producing machine-readable JSON

output for CI pipelines.

— Flag and behavior named but no output example shown

Agentic AppSec on your infrastructure w…

WAS THIS USEFUL?  

Veracode

Feedback

2 RELEASES · 2026-09-10 → 2026-09-12

CHANGELOG ↗

RANK

Veracode is a cloud-based application security platform that performs static, dynamic, and software composition analysis to identify vulnerabilities in code.

> Veracode's window centers on a new Limited-Availability CLI command that auto-remediates SCA findings and IDE/CLI usage analytics, alongside a major Security Labs overhaul: OWASP Top 10:2025 training content, Platform SSO/IAM integration for user management, and several breaking changes retiring legacy eLearning APIs, courses, and terminology.

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

01 **SCA remediation via `veracode fix sca` CLI** NEW 90

Adds the `veracode fix sca` CLI command to analyze vulnerable dependencies surfaced by SCA scans, generate remediation patches, and identify safe upgrade paths. Currently Limited Availability.

After an SCA scan surfaces vulnerable dependencies, automatically generate a remediation patch and safe upgrade path without manually researching fixes.

```
$ veracode fix sca
```

— Names the exact command and its mechanism, includes a runnable example.

changelog-20260912-4d08813d

02 **Get Lesson Progress API enhancements** IMPROVED 90

The Get Lesson Progress API adds an `updatedAfter` parameter for incremental loads, an `excludeNotStarted=true` parameter to filter unstarted lessons, and new `stack` and `updated_on` fields in the response; it now returns a `Not Started` status when both `start_time` and `end_time` are null.

— Names every added parameter, field, and status behavior verbatim.

Training updates (2026-09-10)

03 **OWASP Top 10:2025 training content in Security Labs** NEW 75

Adds full OWASP Top 10:2025 Security Labs curriculum including two new categories, A03 Software Supply Chain Failures and A10 Mishandling of Exceptional Conditions, plus new eLearning courses aligned to OWASP Top 10:2025 for .NET, Java, JavaScript, PHP,

Python, and general Software Security Awareness, available with English, Spanish, French, Portuguese, and Chinese captions.

— Names all new categories, languages, and course scope. Training updates (2026-09-10)

04 **Security Labs default URL change** BREAKING 75

The Security Labs default URL has changed from `https://securitylabs.veracode.com/` to `https://securitylabs.veracode.com/security-labs/`; customers using SSO must update their configured Security Labs URL.

— Gives exact old and new URLs and the required customer action.

Training updates (2026-09-10)

05 **Deprecated legacy training content removed** DEPRECATED 75

Removes 33 deprecated eLearning courses (OWASP 2017, OWASP Top 10 (2021), and Secure Coding for .NET/.Java/.JavaScript/.PHP/.Python, 6 courses each except 3 for Python) and the OWASP Top 10 (2021) Security Labs lessons; certification levels have been updated to include newer replacement courses.

— Enumerates the exact courses and lessons removed and the replacement note.

Training updates (2026-09-10)

THINNER COVERAGE BELOW

06 **Security Labs administration integrated with Veracode Platform**

NEW 55

Integrates Security Labs user and team management with the Veracode Platform, authenticating Security Labs users through Veracode IAM so administrators manage users from a single console under Security Training; adds team search capability for Security Labs administrators and managers.

— Describes the integration mechanism but not a specific API or flag.

Training updates (2026-09-10)

07 **Skills assessment quiz courses** NEW 55

Adds skills assessment quiz courses for Static Analysis, Dynamic Analysis, SCA agent-based scanning, Scan and fix in your IDE, and User and application setup, available in English, Portuguese, and Spanish.

— Lists all five quiz topics and languages, no further mechanism.

Training updates (2026-09-10)

08 **OWASP API Security Top 10 coverage upgraded to 2023** IMPROVED

55

Upgrades OWASP API Security Top 10 coverage in Security Labs from the 2019 list to the 2023 list, adding lessons for three new categories: API 6, API 7, and API 10.

— Names the specific categories added in the upgrade. Training updates (2026-09-10)

---

09 **Security Labs terminology renamed** BREAKING

55

In Security Labs, Teams are renamed to Organizations and Roles are renamed to Teams; any documentation, integrations, or scripts referencing the old terminology must be updated.

— Names the exact terminology change and required follow-up.

Training updates (2026-09-10)

---

10 **IDE and CLI usage analytics dashboard** NEW

50

Adds an IDE and CLI Usage Explore and Dashboard in Veracode Analytics to visualize and explore organization-wide IDE and CLI usage.

— Names the dashboard but gives no metrics or workflow detail.

changelog-20260912-4d08813d

---

11 **Container Security in Docker lesson series** NEW

50

Adds a Container Security in Docker lesson series covering capabilities, users, networking, virtualization, resources, orchestration, and inventory topics.

— Names the lesson topics but no length or format detail. Training updates (2026-09-10)

---

12 **Security Labs lesson UI and admin enhancements** IMPROVED

45

Adds CWE tagging to Security Labs lessons so admins can search lessons by CWE and learners see lessons linked to specific CWEs; adds code syntax highlighting tailored to programming languages in lessons; and adds in-app guidance for creating campaigns and using reporting in Security Labs.

— Groups three thin UI additions with no deeper mechanism given.

Training updates (2026-09-10)

---

13 **Extended eLearning report date range** IMPROVED

35

Extends eLearning report date range selection to up to one year in the past.

— States the new limit with no other mechanism. Training updates (2026-09-10)

14 **eLearning REST API end of support** DEPRECATED 30

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

— States end of support with no migration path given. Training updates (2026-09-10)

15 **Dart, Flutter, and PHP static analysis support** NEW 15

Adds static analysis support for Dart, Flutter, and PHP.

— Only named in the release summary with no elaboration. changelog-20260912-4d08813d

└──▷ **BREAKING ON UPGRADE**

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

! The Security Labs default URL has changed from `https://securitylabs.veracode.com/` to `https://securitylabs.veracode.com/security-labs/` — customers using SSO must update their configured Security Labs URL.

! In Security Labs, Teams are renamed to Organizations and Roles are renamed to Teams — any documentation, integrations, or scripts referencing the old terminology must be updated.

! 33 deprecated eLearning courses (OWASP 2017, OWASP Top 10 (2021), and Secure Coding for .NET/.Java/.JavaScript/.PHP/.Python (6 courses each, 3 for Python)) are no longer available; certification levels have been updated to include newer replacement courses.

! OWASP Top 10 (2021) Security Labs lessons are no longer available following their deprecation.

WAS THIS USEFUL? 👍 👎

Semgrep

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

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

> Semgrep's latest release focuses on API and integration polish: richer Issues API metadata, a new webhook action for Supply Chain incident policies, easier OAuth ticketing reconnection, faster scan startup, and dropped Homebrew support for Intel Macs.

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

01 **Issues API status field descriptions** IMPROVED 60

The Issues API now includes descriptions for the `status`, `triageState`, and `aggregateState` values, and designates `aggregateState` as the recommended field to use.

– Names exact API fields and recommendation, no endpoint path changelog-20260912-8778169c

THINNER COVERAGE BELOW

02 **OAuth ticketing integration reconnection** IMPROVED 35

Semgrep now supports reauthorizing or reconnecting OAuth ticketing integrations without creating a new connection.

– Describes behavior but no integration names or UI path changelog-20260912-8778169c

03 **Faster scan configuration generation** IMPROVED 30

Improved scan configuration generation, starting scans up to 6 seconds sooner.

– Concrete number but no mechanism or config surface changelog-20260912-8778169c

└──▷ **BREAKING ON UPGRADE**

! Homebrew installs of Semgrep are no longer supported on Intel Macs.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Sophos Central Firewall

Feedback ⓘ 1 RELEASE · 2026-09-12

CHANGELOG ↗ RANK

Sophos Central Firewall is a cloud-managed network security solution providing centralized firewall management, threat protection, and policy enforcement across organizations.

> Sophos Central Firewall increased the maximum Firewall Reporting storage entitlement for term-licensed firewall models, allowing more reporting data to be retained before hitting storage limits.

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

01 **Higher Firewall Reporting storage entitlement** IMPROVED

30

For firewall models on term licences, the maximum Central Firewall Reporting storage entitlement has been increased, retaining more reporting data before the storage limit is reached.

– No concrete new limit or figures given, only direction of change

changelog-20260912-7957d66a

WAS THIS USEFUL? 👍 👎

Fastly

Feedback ⓘ 1 RELEASE · 2026-09-01 BLOG ↗ RANK

Fastly is a content delivery network and edge computing platform providing fast, secure content delivery and real-time application performance.

> Fastly added two new Image Optimizer metrics to its analytics and stats APIs for tracking image data volumes.

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

01 **Image Optimizer input/output byte metrics** NEW 65

Fastly's real-time analytics and historical stats API responses now include `imgopto_input_image_bytes` and `imgopto_output_image_bytes`, giving visibility into the input and output data volumes of Image Optimizer traffic.

– Names exact metric fields but no query or dashboard steps given

Add Image Optimizer Input and Output me…

WAS THIS USEFUL? 👍 👎

◆ Network Analysis & Monitoring

Security Onion

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗

RANK

Security Onion is a free and open platform for threat hunting, enterprise security monitoring, and log management. It includes our own interfaces for alerting, dashboards, hunting, PCAP, detections, and case management.

> Security Onion 3.3.0-20260911 adds a pre-upgrade hardware compatibility check to its soup updater.

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

01 **x86-64-v3 CPU check in soup updater** NEW 40

The `soup` updater now runs an x86-64-v3 CPU pre-flight compatibility check to catch incompatible hardware before an upgrade proceeds.

— Names the check and tool but no mechanism details 3.3.0-20260911

WAS THIS USEFUL? 👍 👎

NETRESEC

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

Network forensics, packet sniffers and IT security products. Download NetworkMiner and other free software for network security analysis.

> PolarProxy 2.0.2 adds outgoing SOCKS4/5 tunneling for its proxy connections, new idle- and TLS-handshake timeout controls, environment-variable configuration, an SPDX software bill of materials, and simplified deployment bundles.

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

01 Outgoing SOCKS4/5 proxy tunneling NEW

85

New `--connect socks5:<host>:<port>` (and `socks4` variant) routes PolarProxy's outgoing connections through an upstream SOCKS4 or SOCKS5 proxy, enabling use cases such as decrypting and inspecting your own HTTPS traffic before it is forwarded through Tor.

Intercept and decrypt your own HTTPS traffic before it exits through Tor — useful for auditing what an application actually sends over an anonymizing network.

```
$ PolarProxy --socks 1080 --connect socks5:127.0.0.1:9050 --
nontls allow --pcapoverip 57012 --writeall
```

— Mechanism, use case, and a runnable command are all given changelog-20260912-0f1a6645

02 Idle-connection and TLS handshake timeout flags NEW

80

Adds `--idletimeoutclient <seconds>` and `--idletimeoutserver <seconds>` to close idle/'dead' connections after a configurable period, and `--tlstimeout <seconds>` (default 30s) as a dedicated TLS-handshake timeout separate from the existing TCP-handshake `--timeout <seconds>`.

Kill stalled client and server connections after two minutes of inactivity to prevent zombie sessions from accumulating in long-running deployments.

```
$ PolarProxy --socks 1080 --idletimeoutclient 120 --
idletimeoutserver 120 --tlstimeout 30
```

— Named flags with default value and a runnable example changelog-20260912-0f1a6645

03 Environment-variable configuration support NEW

75

PolarProxy now accepts environment variables as an alternative to command-line arguments, using a `PP_` prefix (e.g., `PP_SOCKS` maps to `--socks`), for cleaner config separation in systemd, Docker, Podman, Kubernetes and Helm deployments via a `polarproxy.env` file; the new `--helpenv` flag prints the full list of supported environment variables.

— Names config keys and file but no runnable example changelog-20260912-0f1a6645

04 **Bundled deployment scripts** NEW 65

Ships with a `docker-compose.yml` for musl builds, or a `systemd` unit file with `install-polarproxy-service.sh` for non-musl Linux builds, to simplify initial deployment.

— Named files give a clear deployment starting point changelog-20260912-0f1a6645

05 **Full PCAP-over-IP output via --writeall** IMPROVED 60

The `--writeall` flag extends PCAP-over-IP output to include all proxied traffic, not just decrypted TLS sessions.

Intercept and decrypt your own HTTPS traffic before it exits through Tor — useful for auditing what an application actually sends over an anonymizing network.

```
$ PolarProxy --socks 1080 --connect socks5:127.0.0.1:9050 --
nontls allow --pcapoverip 57012 --writeall
```

— Flag and before/after named but no dedicated example changelog-20260912-0f1a6645

THINNER COVERAGE BELOW

06 **SPDX software bill of materials** NEW 50

Ships a software bill of materials in SPDX format as `polarproxy.spdx.json`, covering all components, libraries, and dependencies for supply-chain transparency and vulnerability scanning integration.

— Named artifact but no usage steps given changelog-20260912-0f1a6645

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Chainguard

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

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

> Chainguard shipped a Go 1.27 FIPS container image that selects its validated cryptographic module at deployment rather than compile time, alongside 39 new container images added to its catalog this week.

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

01 **Deployment-time FIPS module selection for Go** NEW 80

The new `go-openssl-fips` container image for Go 1.27 selects its FIPS-validated cryptographic module at deployment time rather than at compile time, enabling a single build artifact to run across environments without recompilation. Usage: `FROM cgr.dev/chainguard/go-openssl-fips:latest`.

Build a Go 1.27 FIPS image once and deploy to any environment — the validated OpenSSL FIPS module is chosen at deployment, not compile time, so you no longer need separate pipelines for different FIPS providers.

```
$ FROM cgr.dev/chainguard/go-openssl-fips:latest
```

— Explains mechanism and gives a runnable Dockerfile line changelog-20260912-a78f20e2

THINNER COVERAGE BELOW

02 **39 new container images added to catalog** NEW 50

This week's release adds 39 new container images, including 10 `kubeflow-pipelines-*` FIPS variants and new images for `dbmate`, `hadolint`, `jruby`, `kserve-huggingfaceserver`, `gubernator`, `packer`, `security-profiles-operator`, `aws-lambda-dotnet`, `opentelemetry-go-instrumentation`, `presidio-anonymizer`, `redpanda-console-fips`, and others.

— Names many images but no usage detail per image changelog-20260912-a78f20e2

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

AppOmni

Feedback ⓘ 1 RELEASE · 2026-09-11 BLOG ↗ RANK

Gain complete SaaS visibility, strong posture, and agentic AI governance with AppOmni, the leading SSPM and AISPM platform for enterprises.

> AppOmni expands SSPM into AI-SPM, adding AI Security Posture Management with Agent Inventory, Marlin AI correlation, and the AskOmni conversational assistant for SaaS and AI agent governance.

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

01 **Agent Inventory for AI agents in SaaS** NEW 65

Automatically maps which AI agents exist across the SaaS stack, what they are connected to, and who is using them, covering platforms including Claude, Microsoft 365 Copilot, Salesforce Agentforce, and ServiceNow Now Assist.

Review which AI agents are active in your Salesforce Agentforce environment and what data they can access, using Agent Inventory.

> 📍 In the AppOmni console, navigate to Agent Inventory, filter by platform Salesforce Agentforce, and review agent connections, assigned permissions, and active users.

— Names platforms and includes a console navigation example

AI-Powered Security (2026-09-11)

THINNER COVERAGE BELOW

02 **Marlin AI investigation and correlation** NEW 55

Provides autonomous investigation and correlation, connecting security signals across SaaS and AI ecosystems into a single prioritized view, including prompt injection attempts, high-risk misconfigurations, and ACL role changes, with built-in IP and user behavior analytics.

— Names signal types and analytics but no direct usage steps

AI-Powered Security (2026-09-11)

03 **AskOmni conversational security queries** NEW 45

A conversational interface letting security and IT teams ask plain-language questions to audit an identity, summarize an alert, or generate a remediation script, with one-click connections from active investigations.

— Describes use cases but no concrete command or query example

AI-Powered Security (2026-09-11)

04 **AI Security Posture Management (AI-SPM)** NEW 30

Extends AppOmni's SSPM coverage into AI Security Posture Management, adding capabilities to discover, control, and defend AI agents and copilots running inside SaaS environments.

— Umbrella capability described only at a high level AI-Powered Security (2026-09-11)

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SOAR

Tines

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

Tines lets teams put AI to work across their most sensitive systems, data, and processes, with the security and governance to do it safely.

> Tines' 3B release is a large one: it adds native MCP server configuration, a redesigned monitoring dashboard, git branch management, and well over a dozen new OAuth connectors and AI providers, while also expanding change-control governance and reworking the Cases interface with live updates, a dockable events panel and pinnable columns.

└──▷ **WHAT SHIPPED · 21 FEATURES** most completely described first ? what's the number?

01 **OpenAI-compatible custom AI provider support** NEW 95

Adds an OpenAI-compatible AI provider with support for all auth methods, letting teams point Tines at any OpenAI-compatible endpoint. This supports routing through Amazon Bedrock Mantle by configuring `https://bedrock-mantle.<region>.api.aws/openai/v1` as a custom provider endpoint with API type `OpenAI Responses` and manually adding model IDs such as `openai.gpt-5.6-luna`.

Route Tines AI actions through AWS-hosted OpenAI models via Bedrock Mantle — useful when your org requires all LLM traffic to stay within AWS infrastructure.

> 📍 In Tines, go to Admin › AI › Custom providers › Add provider, set: API endpoint: `https://bedrock-mantle`.<region>.api.aws/openai/v1 API type: OpenAI Responses (under Extra options) Then open the Models tab and manually add a model ID, e.g. openai.gpt-5.6-luna

— Exact endpoint, API type and model ID make this directly runnable. product docs

02 **Workflow monitoring dashboard enhancements** NEW 80

Adds a New Connectors tab in Monitoring for connector observability, a Tines Units drill down, a Set currency option in the Savings tab within Monitoring, a New 'Fix failures' button and New 'Add tests' button on workflow-level monitoring, Jump through step execution failures navigation, and the ability to Set unit tests for workflow steps.

— Names every monitoring surface added but no step-by-step usage shown. product docs

03 **MCP server configuration and access controls** NEW 73

Adds a new MCP settings page for configuring Model Context Protocol integrations, along with Support SSO route auth for MCP servers, MCP support for spaces using git sync, and an option for MCP server connectors to skip authentication.

Navigate to the new MCP settings page to configure Model Context Protocol server connections and toggle authentication requirements.

> 📍 In the Tines console, go to Settings › MCP and configure your MCP server connectors, enabling skip authentication for internal servers as needed.

— Names each MCP capability but no deeper mechanism given. product docs

---

04 **New connectors and OAuth authentication methods** NEW

70

Adds new `OAuth 2.0 connector for ServiceNow`, a `OAuth 2.0 JWT bearer connector`, support for JSON token request format in custom OAuth connectors, and connector status display for OAuth errors with tooltip surfacing. New service connectors include `SendSafely connector`, Greenhouse Harvest v3 OAuth connector, `DatoCMS connector`, `Zscaler OneAPI OAuth connector`, Jira Service Management connector, Gainsight connector with OAuth support, and Productiv connector. Also adds AWS RDS IAM authentication for database connectors and GitHub connector support for GitHub Enterprise Server.

— Names every connector and auth method but no config steps shown. product docs

---

05 **Change control governance enhancements** NEW

65

Adds a Space level block self-approval setting for change control, a warning before pushing live when a link's access scope changed, the ability to rename new stories under change control without requiring approval, and change control comments enabling annotated approval workflows.

— Names each governance control but no step-by-step setup. changelog-20260912-03d32e8a

06 **Audit log search, filtering and retention controls** IMPROVED

65

Adds a Search and filter option to audit logs, and a configurable audit log retention period so teams can control how long audit records are kept.

Review and filter audit log entries by event type to investigate access scope changes before pushing a workflow live.

> 📍 In the Tines console, go to Settings › Audit Logs, then use the Search and filter option to narrow results by event type or user.

— Concrete UI path given for search; retention has no exact config key.

changelog-20260912-03d32e8a

THINNER COVERAGE BELOW

07 **Download workflow as ZIP via API** NEW

55

Adds an API endpoint to download workflow as ZIP for programmatic workflow export.

— Names the endpoint capability but not exact path or method. product docs

08 **Cases interface customization** NEW

50

The events panel can now be docked to keep it persistently visible within the Cases interface, and columns in the cases table can be pinned or hidden to customize the view.

— Names both UI changes but no exact navigation path. product docs

09 **Storage file preview and access** NEW

50

Adds the ability to Preview any file in storage, including audio, video, and markdown, plus the option to View storage from workflow UI.

— Lists file types supported but no navigation detail. product docs

10 **3B assistant gains workflow execution context** IMPROVED

45

3B can now access main branch step executions and past conversations within a workflow context, letting the assistant reference recent runs and prior chat history when helping build or debug workflows.

— Describes capability but no example of use. product docs

11 **Workflow and space discovery navigation** NEW 45

Adds a New Links page to browse links across all spaces, a Discoverable spaces section that collapses in the sidebar, and the ability to Hover to view a workflow README in list.

— Names each surface but no usage walkthrough. product docs

12 **Google Gemini and Microsoft Foundry AI providers** NEW 45

Adds Google Gemini as an AI provider and a Microsoft Foundry connector for accessing Claude and OpenAI models.

— States providers added but no config detail given. product docs

13 **Dashboard draft and edit mode** NEW 40

Adds dashboard draft and edit mode, allowing dashboards to be staged before publishing.

— Describes staging behaviour but no UI path. changelog-20260912-03d32e8a

14 **Security settings page in 3B** NEW 40

Adds a Security settings page with public access and session controls.

— Names the page but not exact controls or fields. product docs

15 **Git branch management for workflows** IMPROVED 40

Adds a Tidy up option for stale branches on a workflow and support so Branches can be renamed.

— Names both additions but no mechanism detail. product docs

16 **Live updates for Cases, Records and dashboards** IMPROVED 35

Cases, Records, and dashboards now stay up to date automatically when open in background browser tabs.

— Describes behaviour but no configuration or limits. product docs

17 **Built-in skills published in public repo** IMPROVED 30

Built-in skills for 3B now live in the public repo for discoverability.

— States location change but no further mechanism. product docs

18 **User preference for default chat AI model** NEW 30

Adds a user preference to set the default chat AI model.

— Names the setting but no location or options listed. product docs

19 **Request to share a connector in 3B** NEW — 25

Adds the ability to request to share a connector in 3B.

— Bare capability name, no workflow detail. product docs

---

20 **Workflow step map redesigned** IMPROVED — 20

The workflow step map view has been redesigned.

— No detail on what changed in the redesign. product docs

---

21 **Case notifications on comment updates** IMPROVED — 20

Sends case notifications when comments are updated.

— Bare statement, no configuration options given. changelog-20260912-03d32e8a

└──▷ **ALSO FROM THESE RELEASES**

.
.
.
.

└──▷ **BREAKING ON UPGRADE**

! Removed endpoint GET `/api`/v1/admin/users/{email}

WAS THIS USEFUL? 👍 👎

◆ SIEM

Databricks

Feedback ⓘ 5 RELEASES · 2026-09-10 → 2026-09-11 BLOG ↗

RANK

Databricks is a unified analytics platform for data engineering, data science, and machine learning built on Apache Spark.

> Databricks' latest releases add a new foundation model, expand OpenSharing to foreign federated tables, give the Jobs API a standard performance mode for one-time runs, and bring Genie AI/BI assistants GA connectors into everyday workplace tools.

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

01 Standard performance mode for one-time Jobs API runs NEW

90

The Jobs API now supports `performance_target` set to `STANDARD` for one-time runs, alongside existing performance targets, to control cost vs. speed trade-offs at submission time. Apache Airflow's `DatabricksSubmitRunOperator` also supports `performance_target: STANDARD` for one-time Databricks job submissions.

Submit a one-time Databricks run with standard performance mode to control cost vs. speed trade-offs at submission time.

```
$ curl -X POST https://<databricks-
instance>/api/2.1/jobs/runs/submit \
  -H 'Authorization: Bearer <token>' \
  -H 'Content-Type: application/json' \
  -d '{"performance_target": "STANDARD", "run_name": "my-one-
time-run", "tasks": [{"task_key": "main", "existing_cluster_id":
"<cluster-id>", "notebook_task": {"notebook_path":
"/path/to/notebook"}}]}'
```

— Names the exact field, value, and includes a runnable submit command

Standard performance mode is now availa…

02 MCP connectors for Genie One and Genie Code NEW

75

Databricks-provided MCP connectors for Google Drive, Gmail, Google Calendar, Microsoft 365, Atlassian, Slack, and GitHub are now generally available, letting Genie One and Genie Code search and act on these external company tools while answering questions. Each user authenticates individually via OAuth so tokens are never shared across users, with access governed through Unity Catalog and Unity Gateway.

— Names all connectors and auth model but no exact setup command

Databricks-provided MCP connectors for …

03 **OpenSharing GA for foreign Iceberg tables and schemas** NEW

60

Databricks OpenSharing is now generally available for sharing objects federated via Lakehouse Federation without copying data: foreign Iceberg tables federated from external Iceberg catalogs can be shared with Delta Sharing recipients, including those using non-Databricks Iceberg clients, and foreign schemas and tables can now be read by recipients through OpenSharing.

— Explains scope and mechanism but gives no setup steps or config

Sharing foreign Iceberg tables with Ope… | Sharing foreign schemas and tables with…

THINNER COVERAGE BELOW

04 **DeepSeek V4.1 Flash on Unity Gateway** NEW

50

Databricks Unity Gateway now supports the DeepSeek V4.1 Flash model, accessible via Foundation Model APIs, with support for text and image inputs.

— Names the model and API surface but no usage example

DeepSeek V4.1 Flash is now available on…

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Elastic Security Labs

Feedback ⓘ 1 RELEASE · 2026-09-11

BLOG ↗ RANK

Power insights and outcomes with The Elasticsearch Platform. See into your data and find answers that matter with enterprise solutions designed to help you accelerate time to insight.

> Elastic Security Labs shipped a layered Linux local-privilege-escalation detection framework, combining several new SIEM and endpoint rules for SUID/SGID abuse and page-cache/COW kernel bugs, plus Auditd Manager guidance and expanded rule coverage mapped to MITRE ATT&CK T1548.001.

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

01 Expanded Linux LPE rule coverage for T1548.001 IMPROVED

77

Extends Elastic prebuilt rule coverage for Linux privilege escalation techniques mapped to MITRE ATT&CK `T1548.001` (Abuse Elevation Control Mechanism: Setuid and Setgid), available in the `detection-rules` repository (SIEM) and the `protections-artifacts` repository (endpoint behavioral rules). Rules can be enabled in Kibana under Security -> Rules -> Detection rules, filtering by tag `OS: Linux` and tag `Tactic: Privilege Escalation`.

Enable all Linux privilege escalation prebuilt rules in Kibana to activate the new SUID/SGID and LPE framework detections across your fleet.

> 📍 In Kibana, go to Security -> Rules -> Detection rules (SIEM), click `Install Elastic rules`, then filter by tag `OS: Linux` and tag `Tactic: Privilege Escalation`, and enable all matching rules.

— Includes exact Kibana navigation and repo names to enable rules

Linux Detection Engineering - Local Pri…

02 SUID helper proxy-execution detection rule NEW

75

New rule inspects `process.args` (rather than `process.name`) for known setuid binary paths — `/usr/bin/pkexec`, `/usr/lib/snapd/snap-confine`, `/usr/bin/newuidmap`, and `/usr/libexec/openssh/ssh-keysign` — combined with `process.args_count <= 2` to catch cases where the helper is passed as an argument to another privileged binary.

— Names all setuid paths and the exact condition used

Linux Detection Engineering - Local Pri…

03 **General outcome-oriented LPE detection rules** NEW 73

New rules key on the common escalation skeleton — an unprivileged process (`uid != 0`) executing from writable paths such as `/tmp` , `/dev/shm` , `/var/tmp` , `/run/user/` , or `/home/` that becomes root — to cover page-cache and no-userland-tell kernel bugs like Copy Fail (CVE-2026-31431) and DirtyFrag (CVE-2026-43284) where no implementation-specific artifact exists.

:
:

— Names writable paths and CVEs shown detected in Kibana

Linux Detection Engineering - Local Pri…

04 **Auditd Manager integration for LPE visibility** NEW 69

Adds guidance for syscall-level LPE visibility via Auditd Manager, requiring `socket` , `splice` , `bind` , and `execve` audit rules to surface the page-cache exploit family including Copy Fail and DirtyFrag.

— Names the exact audit rule set to configure Linux Detection Engineering - Local Pri…

05 **Suspicious SUID/SGID Utility Execution rule** NEW 68

New detection rule combining an euid-0 / non-root-real-user process shape, low `process.args_count` , and an interpreter or writable-path parent to catch abuse of `su` , `sudo` , `pkexec` , and `passwd` with near-zero false positives.

— Names exact fields and binaries but no runnable query given

Linux Detection Engineering - Local Pri…

06 **SUID/SGID binary escalation rule via EQL trick** NEW 65

New rule uses an EQL stringcontains(process.executable, process.command_line) trick to catch abuse of uncommon or long-tail SUID binaries without maintaining a hard-coded name list.

— Mechanism named but not a full runnable rule Linux Detection Engineering - Local Pri…

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Iru

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗ RANK

Manage devices and everything they touch. See how security, IT, and compliance get easier when unified around devices with Iru.

> Iru rolled out Auto Apps for Windows and Mac, added automatic enrollment retry for Return to Service devices, and aligned Compliance Automation with Cyber Essentials.

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

01 **Enrollment retry for Return to Service** NEW 30

Devices can now automatically retry enrollment when using Return to Service, reducing manual re-enrollment steps.

– Explains behavior but lacks configuration specifics What's New in Iru | September 11th

02 **Auto Apps for Windows and Mac** NEW 25

Iru adds Auto Apps support for Windows and Mac devices, letting apps be automatically applied to these platforms.



– Names platforms but no mechanism or config detail What's New in Iru | September 11th

03 **Cyber Essentials alignment in Compliance Automation** IMPROVED 15

Compliance Automation is aligned with Cyber Essentials as part of this release.

– Only mentioned in summary, no detail on mechanism What's New in Iru | September 11th

WAS THIS USEFUL?  

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

runZero is an asset discovery and inventory platform that identifies and maps all devices and software across networks without requiring agents.

> runZero's latest release focuses on access control with custom roles and granular API permissions, adds task reprocessing and SAML certificate expiry alerts to the UI, and rounds out several asset discovery and import fingerprinting improvements.

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

01 **Custom roles and granular API access controls** NEW

58

Custom roles can now be assigned to API keys, default user roles, group permissions, SSO defaults, and MCP connections. Administrators can also create API clients with custom permissions capped by the creator's own access rights, with support for granular authentication scopes on account-level API clients.

— Names several permission surfaces but no exact commands or endpoints

changelog-20260912-24eeaafc

02 **Asset discovery detail improvements** IMPROVED

46

Recent assets now include sub-assets identified through protocol gateways, WS-Discovery `XAddr` endpoints now contribute to asset hostnames, and MAC vendor information is now populated for legacy MAC prefixes.

— Names three concrete discovery mechanisms but no configuration to act on

changelog-20260912-24eeaafc

03 **Cloud and third-party import enhancements** IMPROVED

43

AWS, Azure, and GCP cloud imports now include additional asset types, and Dragos and Wiz imports now apply more complete fingerprinting and OS CPE matching when available.

— Names five integrations but not which new asset types were added

changelog-20260912-24eeaafc

04 **Task summary flag for large asset changes** IMPROVED

36

Task summaries now clearly indicate when a task involved more than 1,000 asset changes.

– Gives a concrete threshold but no further detail on display changelog-20260912-24eeaafc

05 **Task reprocessing from the UI** NEW 26

Tasks can now be reprocessed directly from the user interface.

– Bare description with no navigation detail changelog-20260912-24eeaafc

06 **SAML certificate expiry email warnings** NEW 25

Account administrators now receive email warnings before SAML certificates expire.

– States the alert but no timing or threshold given changelog-20260912-24eeaafc

WAS THIS USEFUL? 👍 👎

Intruder

Feedback ⓘ changelog · Sep 12, 2026 CHANGELOG ↗

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

Intruder: Adds an Additional domains field for web app authentication, allowing subdomains and external services to be included in authenticated scan scope.

└──▷ **HOW TO FIND IT**

When your app at `app.example.com` calls `api.example.com` or an external identity provider, add those domains so the authenticated crawler is not blocked at domain boundaries.

📍 In the target's authentication settings, open the Additional domains field and add the required domains, e.g.: `api.example.com`, `auth.example.com`, `idp.thirdparty.com`

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Okta for AI Agents

Feedback ⓘ 1 RELEASE · 2026-09-12

CHANGELOG ↗ RANK

> Okta shipped a protocol migration for its SAP connector, added a new SCIM integration for Marker.io, and enabled IdP-initiated SSO for Square.

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

01 **Square OIDC IdP-initiated SSO** IMPROVED 30

Square (OIDC) now supports IdP-initiated SSO flow.

— States the flow added but no configuration path given changelog-20260912-30b5a1c1

WAS THIS USEFUL? 👍 👎

ConductorOne

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗

RANK

Govern workforce access, deploy AI agents, and get work done with C1.

> ConductorOne's biggest addition this window is Agent Classifiers, which evaluate AI agent risk at call time and can block, route to human approval, or just log matches in Observe mode; alongside that it shipped new MCP server registration and resource-approval tooling, read-only session-policy preview APIs, expanded system log fields, and a string of smaller governance and role-mining tweaks — plus two breaking changes to automation expressions and the Finding `Owner` field.

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

01 Agent Classifiers for AI agent risk evaluation NEW

90

Agent Classifiers evaluate AI agent risk at call time by writing rules over private-data sensitivity, untrusted-content exposure, and exfiltration capability, then routing matches to a hook, human approval, or block. An Observe mode lets admins log what a rule would catch before turning on enforcement.

Enable Observe mode on an Agent Classifier to log risky tool-call patterns without blocking, so you can tune rules safely before enforcement.

> 📍 In the C1 admin console, go to AI Agents › Classifiers, create or edit a classifier, set the mode to `Observe`, define rules over private-data sensitivity and exfiltration capability, then save — matches are logged but not blocked.

— Full mechanism plus a concrete Observe-mode walkthrough changelog-20260912-87306871

02 Findings 'Owner' field renamed to 'Assignee' BREAKING

80

The `Owner` column, filter, and detail field on Findings are renamed to `Assignee` across the UI, API, webhooks, and audit log; consumers of the Finding object via API, webhook, or SIEM integrations must update field and event-name references accordingly.

— Names every affected surface needing an update changelog-20260912-87306871

03 Configurable bulk request entitlement limit NEW

75

Admins can now set a custom bulk request entitlement limit from Governance > Forms, ranging from 1 to 100 with a default of 10.

Raise the bulk request entitlement cap for high-volume provisioning workflows, such as onboarding, where the default of 10 is too restrictive.

> 📍 In the C1 admin console, go to Governance › Forms, open tenant-wide request settings, and set the max bulk entitlement request limit to a value between 1 and 100.

— Exact range, default, and UI path given `changelog-20260912-87306871`

---

04 **Automation expressions require static field paths** BREAKING

75

Automation expressions that reference the bare workflow context, or pass it directly to a function, no longer compile — each expression must name the step and field directly. Already-running automations are unaffected until next edited and saved, at which point indirect-reference expressions must be rewritten to a static path.

— Explains trigger condition and required migration `changelog-20260912-87306871`

---

05 **Expanded system log event fields and classes** IMPROVED

70

System log events now include a `groups[]` field and `correlation_uid`, plus four new Identity & Access event classes: Account Change, Entity Management, User Access Management, and Group Management. Machine identities are now reported as the `Service` account type in these logs.

— Names exact fields and event classes but no query example `changelog-20260912-87306871`

---

06 **Resource approval tab for MCP servers** NEW

65

A new Resources tab for MCP servers lets admins review and approve static resources and URI templates discovered by C1; each approved resource gets its own read entitlement, governed separately from tool and toolset access.

— Explains mechanism and entitlement separation clearly `changelog-20260912-87306871`

---

07 **Connector sync failing finding type** NEW

65

A new `Connector sync failing` finding type triggers after two consecutive failed full syncs and auto-resolves on the next successful sync; it can be disabled per tenant.

— States trigger condition, resolution, and disable option `changelog-20260912-87306871`

---

08 **Role mining shared-access and approval routing** IMPROVED

60

Role mining gains a shared-access threshold setting, pre-action entitlement list fine-tuning, and optional routing of automatic profile enrollments through an access request

task for approval.

— Names three additions but no exact settings paths changelog-20260912-87306871

THINNER COVERAGE BELOW

09 **Session policy preview API endpoints** NEW 55

Four new read-only API endpoints let admins preview which session policy applies to a given user — by direct assignment, group membership, or tenant default — and list every user a policy applies to, including group-conferred access with the conferring group named.

— Mechanism explained but endpoint methods/paths not named changelog-20260912-87306871

10 **Guided MCP server registration flow** IMPROVED 55

MCP server registration now uses a guided step-by-step flow covering server identity, hosting location, URL, access controls, tool discovery behavior, and authentication.

— Names flow steps but no exact fields or defaults changelog-20260912-87306871

11 **Same-app entitlement bindings** NEW 55

The entitlement binding picker now includes entitlements from the same app, enabling same-app bindings such as Salesforce Admin -> Salesforce Editor.

— Concrete example given, no config key named changelog-20260912-87306871

12 **Access-request duration and suspension visibility** IMPROVED 45

Access-request flows now display the entitlement's duration limit up front and flag when the target user, or the holder of already-granted access, is suspended.

— Describes UI behavior, no config surface named changelog-20260912-87306871

13 **Reorderable provisioning steps** IMPROVED 45

Provisioning steps on an entitlement can now be reordered in place — moved up or down directly — without removing and re-adding them.

— Clear UI action but no exact path specified changelog-20260912-87306871

14 **Auto-created API credential on device registration** NEW 40

Registering a new desktop device now auto-creates a full-access API credential, displayed on the registration success screen.

— Describes behavior but no scope or config detail changelog-20260912-87306871

└──▷ **BREAKING ON UPGRADE**

! Automation expressions that reference the bare workflow context, or pass it directly to a function, no longer compile — each expression must name the step and field directly. Automations already running are unaffected until next edited and saved, at which point indirect-reference expressions must be rewritten to a static path.

! The `Owner` column, filter, and detail field on Findings are renamed to `Assignee` in the UI, API, webhooks, and audit log — consumers of the Finding object via API, webhook, or SIEM integrations must update field and event-name references accordingly.

WAS THIS USEFUL? 👍 👎

Clerk

Feedback ⓘ **1 RELEASE · 2026-09-12** **CHANGELOG ↗** **RANK**

The easiest way to add authentication and user management to your application. Purpose-built for React, Next.js, Remix, and “The Modern Web”.

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

01 **OAuth 2.0 Device Authorization Grant (beta)** **NEW** 75

Clerk now supports the `device_authorization_endpoint` and grant type `urn:ietf:params:oauth:grant-type:device_code`, automatically advertised via OAuth 2.0 and OpenID Connect metadata when the Device Authorization Grant is enabled. Clerk's Account Portal hosts user verification for device flows, displaying the OAuth application, requested scopes, an optional Organization selection, and approve/deny actions.

⋮

— Names endpoint and grant type but no enablement flag shown `changelog-20260912-8dea503f`

└──▷ **BREAKING ON UPGRADE**

! Deprecated endpoint DELETE `/users`/{user_id}`/trusted`_devices/{trusted_device_id} (still works)

! Deprecated endpoint GET `/users`/{user_id}`/trusted`_devices (still works)

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ 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 biggest window shipped a full Password Vault rollout across mobile, Admin Portal, User Portal, and the JumpCloud Go browser extension, plus Public Preview Agent Identities for non-human AI agents, GA Access Risk Detection, a new Custom Query Builder for reporting, and MCP/AI Gateway discovery and app-assignment changes.

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

01 **Agent Identities for non-human AI agents** NEW 85

New `Identity Management > Agents` section (Public Preview) lets admins register and govern non-human AI agent identities with OAuth client credentials, grant group-based SSO application access via Agent Groups, and manage their lifecycle independent of human user accounts.

Register a new AI agent identity with OAuth credentials so an AI agent can access SSO applications without sharing a human user account.

> 📍 In the Admin Portal, go to Identity Management › Agents and click + Add. On the Details tab, enter the agent name, owner, and company email. On the Authentication tab, click to generate OAuth client credentials for the JumpCloud AI Gateway. Then go to Identity Management › Agent Groups, create a group, add the agent, and assign the required SSO applications.

— Exact navigation and step-by-step setup given in usage example

changelog-20260912-6fcef65f

02 **Custom Query Builder in Insights Reports** NEW 80

New `Insights > Reports` section adds a Custom Query Builder supporting manual report building and natural-language queries, filter operators (Equals, Contains, Is Null), and export in CSV and JSON formats with scheduling.

Build a custom report of all inactive user accounts and export it as JSON for ingestion into a SIEM or audit workflow.

> 📍 In the Admin Portal, go to Insights › Reports and open the Custom Query Builder. Select the user entity, add a filter using the Is Null operator on last-login date, choose your display columns, then export the result as JSON.

— Names operators and export formats with a runnable example changelog-20260912-6fcef65f

03 **Access Risk Detection (GA)** NEW 75

Access Risk Detection is now GA, providing behavior-based detection of unusual locations, impossible travel, unfamiliar devices/browsers, dormant accounts, and abnormal login volumes across the Admin Portal, User Portal, managed device logins, and SSO applications. It supports customizable risk factors, automatic MFA-based resolution, intelligent VPN/gateway suppression, and email, Slack, and webhook notifications.

— Rich mechanism and scope but no exact config path given changelog-20260912-6fcef65f

04 **MCP Discovery and token/cost tracking on managed devices** NEW 75

Device settings gain MCP Discovery and Token & Cost Tracking options under Enhanced Discovery Options, surfacing MCP servers and token/cost data from Cursor, Claude Code, OpenCode, Codex, VS Code, and Copilot CLI on managed Windows and macOS devices.

Enable MCP server discovery and AI token cost tracking on managed devices to surface shadow AI tool usage across your fleet.

> 📍 In the Admin Portal, go to device management settings. Under Enhanced Discovery Options, select MCP Discovery and Token & Cost Tracking, then save.

— Names the exact toggle location and supported tools with steps

changelog-20260912-6fcef65f

05 **MCP server SSO app assignment now required** BREAKING 75

MCP servers previously created without an associated SSO application or bookmark now require one to be assigned in AI Gateway; access is no longer scoped by User Groups until an application is assigned. The custom app creation option has been removed from the Add MCP Server dialog — a `+ New App` button now launches the standard Add New SSO Application wizard during server setup instead.

— Clear before/after and the replacement UI control are named changelog-20260912-6fcef65f

06 **Password Vault management in Admin Portal** NEW 70

Admin Portal now includes Password Vault management: vault enablement, user/group enrollment, permission management (Connect, View, Edit, Manage), credential sharing, and password health monitoring via an Overview dashboard. Password Vault audit log entries were also added to Directory Insights.

— Names permission levels and dashboard but only a UI path, no exact steps

changelog-20260912-6fcef65f

07 **Device Trust for third-party MDM-managed mobile devices** NEW

70

Device Trust and conditional access policy support now extends to mobile devices managed by third-party MDMs (e.g., Jamf, Kandji, Google Workspace EMM), registered via a shared secret with an SSO Extension profile in the existing MDM.

— Names MDM vendors and registration mechanism, no exact steps

changelog-20260912-6fcef65f

08 **Password Vault autofill via JumpCloud Go extension** NEW

65

The JumpCloud Go browser extension gains Password Vault autofill, supporting launch-and-autofill for non-SSO websites and 2FA codes, credential secret viewing, and save-on-login/update/signup — with no device registration required.

— Explains mechanism and scope but no exact command or config changelog-20260912-6fcef65f

09 **Password Vault in User Portal** NEW

60

Password Vault is now available in the User Portal left navigation, supporting credential and website management, sharing with Connect, View Secret, View Detail, and Manage permissions, and bulk import via CSV or Excel.

— Names import formats and permission levels, only a UI path given

changelog-20260912-6fcef65f

THINNER COVERAGE BELOW

10 **Password Vault in JumpCloud Protect mobile app** NEW

45

Password Vault is now in the JumpCloud Protect mobile app, enabling autofill in mobile apps and the mobile browser, and viewing shared credentials and folder contents from the Password Vault tab.

— Describes capability but only a bare UI location, no steps changelog-20260912-6fcef65f

11 **Admin access requests from Menu Bar and Tray apps** NEW

40

Admins can now create access requests directly from the JumpCloud Menu Bar (Mac) and JumpCloud Windows Tray app, without requiring access to the full User Portal.

— Names the exact apps but gives no step-by-step flow changelog-20260912-6fcef65f

12 **Password Vault audit log entries in Directory Insights** NEW

25

Password Vault activity now generates audit log entries in Directory Insights.

— One-line addition with no mechanism or navigation detail changelog-20260912-6fcef65f

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! MCP servers previously created without an associated SSO application or bookmark now require one to be assigned in AI Gateway; access is not scoped by User Groups until an application is assigned.

! The custom app creation option has been removed from the Add MCP Server dialog; a new application must be created via `+ New App`, which opens the standard Add New SSO Application wizard.

WAS THIS USEFUL? 👍 👎

Okta Identity Engine

Feedback

1 RELEASE · 2026-09-10

BLOG ↗ RANK

Secure, scalable, and highly available authentication and user management for any app.

> Okta Identity Engine's September window adds governance APIs (cancel-request endpoints, higher Access Request limits, GA certification APIs), stronger network defenses (malware proxy detection, PowerShell-driven AD automation), and expanded authentication options (NFC authenticator support, passkey enrollment prompts, configurable refresh token lifetimes for Native-to-Web SSO).

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

01 **Cancel-request APIs for Access Requests** NEW 85

Adds three new cancel-request API endpoints — Update a request (Access Request V1), Update a request (Requests V2), and Update my request (My Requests) — in Beta, enabling programmatic cancellation of active and pending access requests from custom portals, ITSM tools, CLIs, or chatbots.

— Three endpoints named, but no request/response schema shown. product docs

02 **Malware proxy detection and IP reputation feeds in dynamic zones**

NEW 85

Adds a `MALWARE_PROXIES` IP service category to enhanced dynamic network zones, powered by Okta CyberDefense, covering proxy services linked to malware and botnet activity (including 911 S5, NSOCKS, iProxy, and BHProxies), now GA in Production. Also adds a new IP Service for enhanced dynamic network zones allowing zone policies to reference dynamically updated IP reputation feeds.

Block traffic from malware-associated proxy networks by adding the `MALWARE_PROXIES` service to a dynamic network zone.

> 📍 In the Admin Console, go to Security › Networks, open or create an Enhanced Dynamic Zone, expand IP Services, and enable `MALWARE_PROXIES` to block proxy IPs linked to botnets and malware (including 911 S5, NSOCKS, iProxy, BHProxies).

Enable the Malware Proxies IP Service on a dynamic network zone to automatically deny sign-in attempts routed through known malware proxy infrastructure.

> 📍 In the Admin Console, go to Security › Networks, open or create a Dynamic Zone, and under IP Services enable Malware Proxies, then save the zone policy.

— Named service and provider, plus exact admin console steps.

Monthly release 2026.09.0 (2026-09-10)

03 **PowerShell script execution for on-prem Active Directory** NEW

85

Enables admins to execute custom PowerShell scripts in on-premises Active Directory environments via the Active Directory agent, invokable through Okta Workflows and the Okta public API `Invoke a remote script on the AD agent`; now GA in Preview.

— Named API operation and invocation paths, no sample script.

Monthly release 2026.09.0 (2026-09-10)

04 **Telephony inline hook payload fields** NEW

80

Adds `data.context.app.clientId` and `data.messageProfile.isResend` fields to the telephony inline hook request payload, identifying the signing-in app and whether an OTP is a resend within the same session.

Detect whether an OTP was resent in the same session inside a telephony inline hook handler, so you can apply rate-limiting or alerting logic.

json

```
{
  "data": {
    "context": {
      "app": {
        "clientId": "0oabc123def456"
      }
    },
    "messageProfile": {
      "isResend": true
    }
  }
}
```

— Exact field names and a runnable example payload provided.

Monthly release 2026.09.0 (2026-09-10)

05 **Search, filter, and export on the Applications page** NEW

80

Adds search by name or client ID, filter by type and status, a last-modified-date view, and CSV export to the Applications page, with programmatic access via the `List all applications that match search filters` API; available as Early Access.

Export the full application catalog from the Applications page for an access review or audit, without scripting an API call.

📍 In the Admin Console, go to Applications › Applications, use the search and filter controls to scope the list, then click `Export` to download the results.

— Named API and exact UI navigation for export. Monthly release 2026.09.0 (2026-09-10)

06 **Higher Access Request configuration limits** IMPROVED

70

Increases Access Request limits: users per task or question raised to 25 (from 10), entitlement bundles in an access level condition to 1,000 (from 100), groups in an access level condition to 1,000 (from 500), request type configuration lists per org to 250 (from 100), and request types per org to 750 (from 500).

— Precise before/after numbers, but no config surface named. product docs

07 **NFC authenticator and passkey enrollment enhancements** NEW

60

Adds NFC authenticator support (self-service Early Access in Preview), enabling NFC-based hardware tokens as an authentication factor. Adds `transports` values to WebAuthn authenticator enrollments (GA in Preview), exposing the physical transport (USB, NFC, BLE, internal) used during passkey registration. Supports prompting users to enroll a passkey during sign-in flows (GA in Preview), increasing passkey adoption without requiring admin-forced enrollment.

— Named field and factor types, but no config or API path given.

Monthly release 2026.09.0 (2026-09-10)

THINNER COVERAGE BELOW

08 **Configurable refresh token lifetimes for Native-to-Web SSO**

IMPROVED

45

Refresh token lifetimes in Native to Web SSO flows are now configurable and GA in Production, giving admins control over session continuity across native and web app handoffs.

— States the capability but not the config field or defaults.

Monthly release 2026.09.0 (2026-09-10)

09 **GA for campaign decisions and AI agent certification APIs**

IMPROVED

40

API support for Access Certification campaign decisions is now GA in Production, and Certify AI agent resource connections is now GA in Production.

— Bare GA announcements with no mechanism or usage detail. product docs

10 **Dynamic Client Registration API** NEW

40

Adds API support for Dynamic Client Registration (Beta), allowing OAuth clients to register programmatically without manual admin configuration.

— No endpoint name or parameters given, just prose.

Monthly release 2026.09.0 (2026-09-10)

11 MCP server registration in Integration Network NEW

40

Adds Okta Integration Network MCP server registration (Beta), enabling MCP servers to be registered and managed within the Okta Integration Network.

— No endpoint or workflow detail beyond a one-line description.

Monthly release 2026.09.0 (2026-09-10)

WAS THIS USEFUL?  

Didit

Feedback

ⓘ

1 RELEASE · 2026-09-12

CHANGELOG ↗

RANK

Didit provides identity verification, fraud prevention, and transaction-monitoring APIs, SDKs, and MCP tools.

> Didit's biggest release of the window adds a non-document Data match identity verification method with per-country controls, plus new result fields exposing verification method, assurance tier, and registry comparison details.

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

01 Per-country ID verification method controls

NEW

86

Adds per-country method controls via the Countries tab on the ID Verification step, toggleable through both the console and the API. To enable, open workflow > ID Verification step > Countries tab, toggle Data match on for the target country, set the fallback for No match to Document capture or Decline, and set retries (1–5); the console displays the per-lookup cost before confirming.

Enable non-document lookup for a specific country so users can verify without uploading a photo — useful for markets where document capture has high drop-off.

> 📍 In the console, open your workflow › ID Verification step › Countries tab. Find the target country, toggle Data match on, set the fallback for No match to Document capture or Decline, and set retries (1–5). Save — the console shows the per-lookup cost before you confirm.

— Exact console navigation and settings make this directly runnable

changelog-20260912-63eeeaf3

02 Verification method and assurance tier fields

NEW

67

Sessions, the decision API, and the `status.updated` webhook now carry the method that produced each ID Verification (`document`, Data match, or wallet) and its assurance tier (Documentary, Data match, or Cryptographic).

— Names exact API surfaces and field values, no usage example given

changelog-20260912-63eeeaf3

03 Automatic liveness and face match for portrait-issuing registers

NEW

66

Where a government register returns a portrait (South Africa, Nigeria, Argentina, Panama), a Data match lookup automatically adds passive liveness and face match at no extra charge, allowing downstream Liveness and Face Match steps to be skipped.

— Names countries and behaviour but no config key to control it

changelog-20260912-63eeeaf3

04 **"Data match" non-document ID verification method** NEW

62

Didit adds Data match as a new ID Verification method: users enter a national ID number and personal details, which are checked against government registers, credit bureaus, or utility/residential records — no photograph or document upload required.

— Names data sources and mechanism but no API surface for this method itself

changelog-20260912-63eeeaf3

THINNER COVERAGE BELOW

05 **Registry comparison result fields** NEW

50

Adds Registry comparison result fields showing every compared field, the value the user provided, the value the source held, and whether it matched.

— Describes fields but no endpoint name or worked example changelog-20260912-63eeeaf3

WAS THIS USEFUL?  

◆ Secure Access (VPN / SASE / ZTNA)

OpenVPN

Feedback ⓘ 1 RELEASE · 2026-09-11 BLOG ↗ RANK

OpenVPN is an open source VPN daemon

> OpenVPN launched Access Server Link, a guided browser-based deployment path for self-hosted ZTNA on AWS, Azure and Google Cloud with automatic SSL and DNS handling, alongside a new Zero Trust Application Broker for per-application isolation.

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

01 **Access Server Link guided ZTNA deployment** NEW 80

Access Server Link is a new guided, browser-based setup available from Access Server Hub that deploys self-hosted Access Server instances on AWS, Azure, or Google Cloud using only three inputs — hostname, cloud provider/region, and admin password — without SSH, manual DNS configuration, or certificate management. It automatically provisions and renews SSL certificates, replacing self-signed certificates and eliminating certificate-expiry outages, and detects cloud IP changes to update domain records automatically so deployments stay reachable without manual DNS intervention.

Deploy a self-hosted Access Server instance on AWS, Azure, or GCP without SSH or manual DNS work — get ZTNA running in minutes from Access Server Hub.

📍 In Access Server Hub, select Deploy with Access Server Link, choose your cloud provider (AWS, Azure, or GCP) and region, enter a hostname and admin password, then launch — DNS and SSL certificates are provisioned automatically.

— Names exact inputs and setup steps but no CLI or API surface launch-20260911-48845bcc

THINNER COVERAGE BELOW

02 **Zero Trust Application Broker for per-app access** NEW 50

A new Zero Trust Application Broker mediates per-application access using placeholder IP addresses scoped to a single authorized application configured by domain name, making lateral movement between applications structurally impossible.

— Explains mechanism but gives no config surface or command launch-20260911-48845bcc

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

RegScale

Feedback ⓘ 1 RELEASE · 2026-09-11 BLOG ↗ RANK

RegScale is a compliance and security management platform that automates regulatory assessments and governance workflows for organizations.

> RegScale's CLI 6.45.10 adds explicit-suppression support to JCAM import configuration, letting tenants mark excluded fields as intentional rather than silently dropped.

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

01 **@drop value for JCAM config fields** NEW 75

The CLI now accepts `@drop` as a value for `jcamPositionRoleNames` and `jcamAgencyDefinedDataItems` in JCAM profile config, allowing tenants to explicitly record that a point of contact or agency-defined attribute is intentionally excluded from import rather than silently omitting it.

Explicitly suppress a point-of-contact role and an agency-defined attribute during JCAM import, making the exclusion auditable rather than invisible.

yaml

```yaml
jcamPositionRoleNames:
  - "@drop"
jcamAgencyDefinedDataItems:
  - "@drop"
```

— Names exact config keys and value, with runnable YAML example. CLI 6.45.10 (2026-09-11)

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

ai-safe2-framework

Feedback ⓘ 1 RELEASE · 2026-09-11

NOTES ↗ RANK

Ai-Safe2-Framework provides governance, risk, and compliance controls for securing agentic AI systems and non-human identities.

> SAFE2 CLI 0.3.0 introduces a full `feedback` subcommand suite for capturing, verifying, and signing evidence from AI agent task runs, alongside versioned JSON contracts to support automating those workflows.

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

01 **Evidence receipts for agent task claims** NEW 81

`safe2 feedback receipt` produces JSON or Markdown evidence receipts for AI agent task claims, configurable via `--artifact-root`, `--format`, and `--output` options.

— Names command and three flags with exact formats 2026-09-11_safe2_CLI_0.3.0

02 **Pytest evidence capture and offline verification** NEW 77

`safe2 feedback capture-pytest` runs selected tests and captures fresh evidence, recording the observed exit code and test results separately from overall process success. `safe2 feedback verify-pytest` rechecks a saved pytest capture offline, recomputing hashes and test assessments without re-executing the tests.

— Explains mechanism for both commands, no flags given 2026-09-11_safe2_CLI_0.3.0

03 **Detached signing and verification of reports** NEW 68

`safe2 feedback sign-report` creates a detached signature authenticating test/tool report bytes against an operator-trusted key, and `safe2 feedback verify-report` checks a detached signature against a supplied trusted key.

— Names both commands and signing mechanism, no flags 2026-09-11_safe2_CLI_0.3.0

THINNER COVERAGE BELOW

04 **Per-task resource usage correlation** NEW 52

`safe2 feedback usage` correlates declared per-task resource use, separating reported, estimated, and unknown values.

— Names command and its three-way value split 2026-09-11_safe2_CLI_0.3.0

05 **JUnit XML import into SAFE2 evidence format** NEW 45

`safe2 feedback import-junit` normalizes supported JUnit XML reports into the SAFE2 evidence format.

— Bare description of a single command `2026-09-11_safe2_CLI_0.3.0`

---

06 **Versioned JSON contracts for evidence automation** NEW

29

SAFE2 CLI exposes seven versioned JSON contracts to support automation of evidence receipts and test/tool report workflows.

— Mentions a count but no schema names or endpoints `2026-09-11_safe2_CLI_0.3.0`

WAS THIS USEFUL? 👍 👎

NoLabs nono

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗ CODE ↗

RANK

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

> nono's biggest changes this window are a breaking cleanup that strips out legacy CLI flags, environment variables, profile keys and the `nono policy` / `nono prune` subcommands, alongside new session lifecycle management commands and an internal bootstrap improvement for network-notification sessions.

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

01 Removal of legacy profile and CLI aliases

BREAKING

85

v0.77.0 removes all legacy profile-key aliases and CLI flag aliases — including `--allow-net`, `--net-allow` — and environment variable aliases `NONO_NET_BLOCK`, `NONO_NET_ALLOW`, `NONO_ALLOW_PROXY`, `NONO_PROXY_ALLOW`, `NONO_PROXY_CREDENTIAL`, `NONO_EXTERNAL_PROXY`, `NONO_EXTERNAL_PROXY_BYPASS` — which now fail to parse instead of warning. The `nono policy` subcommand and its sub-forms (`nono policy groups`, `nono policy profiles`, `nono policy show`) are removed in favor of `nono profile` equivalents; the `nono prune` subcommand is removed entirely; and profile JSON keys `security.allowed_commands` and `policy.add_deny_commands` are no longer accepted, replaced by `commands.allow` and `commands.deny` respectively.

— Enumerates every removed flag, env var, subcommand and key with replacements v0.77.0

02 Session lifecycle management commands NEW

75

nono adds session lifecycle management for live sandbox sessions via `nono session ps`, `attach`, `detach`, `stop`, `inspect`, and `nono session cleanup` subcommands, allowing operators to list, connect to, and remove sessions from the CLI runtime. Cleanup should be used carefully against paused or stopped sessions until conservative handling is tightened.

Clean up terminated sessions from the nono runtime — note: avoid running against paused/stopped sessions until conservative handling is tightened.

```
$ nono session cleanup
```

— Names all six subcommands with one runnable example product docs

THINNER COVERAGE BELOW

03 CLONE_FILES bootstrap for network-notification sessions

IMPROVED

45

Network-notification session bootstrap now uses `CLONE_FILES`, improving session startup for that session type.

— Names the mechanism but gives no reader-facing action v0.77.0

└──▷ **BREAKING ON UPGRADE**

! The `nono policy` subcommand (and all its sub-forms such as `nono policy groups`, `nono policy profiles`, `nono policy show`) is removed — use `nono profile` equivalents instead.

! Legacy profile keys and CLI flag aliases (`--allow-net`, `--net-allow`, and others) and environment variable aliases (`NONO_NET_BLOCK`, `NONO_NET_ALLOW`, `NONO_ALLOW_PROXY`, `NONO_PROXY_ALLOW`, `NONO_PROXY_CREDENTIAL`, `NONO_EXTERNAL_PROXY`, `NONO_EXTERNAL_PROXY_BYPASS`) are removed and now fail to parse — replace with their current equivalents.

! The `nono prune` subcommand is removed from the CLI.

! Profile JSON keys `security.allowed_commands` and `policy.add_deny_commands` are no longer accepted — use `commands.allow` and `commands.deny` respectively.

WAS THIS USEFUL?

ToolHive

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗ RANK

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

> ToolHive v0.49.0 introduces a per-backend dial-control policy for MCP session networking, an explicit OAuth2 token endpoint auth method, and a new generated Go management API client, alongside breaking changes to AWS STS role claim handling and a bumped Go toolchain requirement.

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

01 Per-backend dial-control policy

BREAKING

90

`session.WithDialControlResolver` in `pkg/vmcp/session` replaces `session.WithDialControl`, allowing different network dial policies to be applied per workload ID instead of a single global policy (e.g. blocking private-range access for most workloads while permitting it for a trusted internal service). The older `session.WithDialControl` is removed, so call sites must migrate to the new resolver or the build fails with `undefined: session.WithDialControl` (the identically-named `pkg/vmcp/client.WithDialControl` is unchanged).

Apply a per-backend dial-control policy so private-range access is blocked for most workloads but permitted for a trusted internal service.

go

```
factory := session.NewSessionFactory(registry,
    session.WithDialControlResolver(
        func(workloadID string) func(string, string,
syscall.RawConn) error {
            if allowsPrivateDialing(workloadID) {
                return nil
            }
            return denyPrivateRanges
        },
    ),
)
```

— Full mechanism, migration path, and runnable code example included. v0.49.0

02 Explicit OAuth2 token endpoint auth method

BREAKING

85

Adds `tokenEndpointAuthMethod` / `token_endpoint_auth_method` field to `oauth2` upstream provider config, letting operators explicitly select `client_secret_basic` or POST-body credential delivery per upstream. Upgrading from v0.48.0, a pre-registered `oauth2` upstream with a client secret and no explicit `tokenEndpointAuthMethod` now reverts from `client_secret_basic` back to POST-body delivery, so IdPs requiring HTTP Basic must set `tokenEndpointAuthMethod: client_secret_basic` explicitly.

Opt a pre-registered OAuth2 upstream into HTTP Basic authentication at the token endpoint when your IdP requires it.

yaml

```yaml
upstreamProviders:
  - name: my-idp
    type: oauth2
    oauth2Config:
      clientId: my-client
      clientSecretRef:
        name: idp-client-secret
        key: client-secret
      tokenEndpoint: https://idp.example.com/oauth2/token
      tokenEndpointAuthMethod: client_secret_basic
```

— Names field, accepted values, and exact migration requirement. v0.49.0

03 **Go 1.27 toolchain requirement** BREAKING 65

The root Go module now requires Go 1.27; builds pinned to Go 1.26 via `GOTOOLCHAIN=local` will fail with `go: go.mod requires go >= 1.27`. The `go://` workload default builder image moves from `golang:1.26-alpine` to `golang:1.27-alpine`.

— Names exact versions and error message, no remediation steps. v0.49.0

04 **AWS STS role claim matching fixed** BREAKING 60

AWS STS role claims of type object, number, boolean, or null now fail closed with HTTP 403 instead of silently granting the fallback role, and a bare-string claim that exactly matches a configured `claim` now selects its mapped role instead of `fallbackRoleArn`.

— Describes behavior change but gives no config example. v0.49.0

THINNER COVERAGE BELOW

05 **Generated Go client for management API** NEW 10

ToolHive now ships a dependency-light generated Go client for the management API.

— Only mentioned in summary, no further detail given. `v0.49.0`

└──▷ **BREAKING ON UPGRADE**

! `session.WithDialControl` in `pkg/vmcp/session` is removed; call sites must be migrated to `session.WithDialControlResolver` or the build fails with `undefined: session.WithDialControl`. Note: the identically-named `pkg/vmcp/client.WithDialControl` is unchanged.

! OAuth2 upstream `tokenEndpointAuthMethod` default is reverted: upgrading from v0.48.0 with a pre-registered `oauth2` upstream that had a client secret and no explicit `tokenEndpointAuthMethod` reverts from `client_secret_basic` back to POST-body credential delivery; IdPs that require HTTP Basic must now set `tokenEndpointAuthMethod: client_secret_basic` explicitly.

! AWS STS role claims of type object, number, boolean, or null now fail closed with HTTP 403 instead of silently granting the fallback role; a bare-string claim that exactly matches a configured `claim` now selects its mapped role instead of `fallbackRoleArn`.

! The root Go module now requires Go 1.27; builds using `GOTOOLCHAIN=local` pinned to Go 1.26 will fail with `go: go.mod requires go >= 1.27`. The `go://` workload default builder image moves from `golang:1.26-alpine` to `golang:1.27-alpine`.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

joplin

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗ RANK

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

> Joplin v3.7.18 adds a small whiteboard usability improvement, letting users double-click to create a note.

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

01 **Double-click to add note on whiteboard** NEW 40

Double-clicking an empty whiteboard canvas now adds a note directly, instead of requiring a separate creation step.

— Describes the action but no further mechanism detail v3.7.18

WAS THIS USEFUL? 👍 👎

Obsidian

Feedback ⓘ 1 RELEASE · 2026-09-12 CHANGELOG ↗ RANK

The free and flexible app for your private thoughts.

> Obsidian's latest update focuses on iOS Quick Capture location targeting, an upgrade to MathJax 4.1.3 for math rendering, system text-size accessibility scaling, and right-to-left support in Bases table views.

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

01 **Location targeting for iOS Quick Capture** NEW 70

iOS Quick Capture gains location awareness across several surfaces: templates can insert the `{{openStreetMapLink}}` variable to link the user's current position, a configurable Home Screen widget on iOS 26 offers shortcuts to capture directly to different Locations, Lock Screen and Control Center Quick Capture widgets can be configured to open a specific Location, and the Quick Capture action in Shortcuts now supports a Location parameter.

– Names widget surfaces and template variable but no full setup steps changelog-20260912-0c58d438

02 **System text-size scaling for interface and text** NEW 70

Text and interface elements now scale with the system's preferred text size, including larger accessibility sizes. A new `--font-preferred-size` CSS variable combines `--font-text-size` with the `--preferred-text-scale` multiplier for text that should respect the system preferred text size on mobile.

– Names exact CSS variables theme authors can use changelog-20260912-0c58d438

THINNER COVERAGE BELOW

03 **Math rendering upgraded to MathJax 4.1.3** IMPROVED 50

Math rendering now uses MathJax 4.1.3, replacing the previous MathJax 3 and Temml renderers.

– Clear before/after but no user-facing action required changelog-20260912-0c58d438

04 **Right-to-left support in Bases table views** NEW 45

Bases table views now support right-to-left (RTL) layouts, including keyboard navigation, selections, and horizontal scrolling.

– Describes scope but no config or command to invoke it changelog-20260912-0c58d438

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 12, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue