THE CYBER TOOLCHAIN NO. 069

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 9, 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 312 changes

Do you prefer **scroll**?

▸ // CONTENTS SHOW 44 of 45 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. Velociraptor can now parse ADCS certificate databases straight off disk, so ESC-style certificate abuse is

vim ? help

huntable without touching the CA. getsploit v3 runs exploit search fully offline from a local SQLite FTS5 index. And ConductorOne's agent classifiers inspect MCP tool calls for sensitive data and exfiltration risk.

DETECT

Hunt certificate abuse from the CA's own database

Velociraptor's new artifact parses Active Directory Certificate Services databases directly from disk, so an analyst can look for rogue templates and abusive enrollments without a live CA query or vendor tooling. Hayabusa's `sort-csv` sorts, dedupes and merges scan output across files or whole directories, which is the tedious part of turning a multi-host sweep into one timeline.

Velociraptor · Hayabusa

GOVERN

Put a policy check in front of what AI agents are allowed to touch

ConductorOne's classifiers evaluate MCP tool calls for data sensitivity and exfiltration risk rather than trusting the agent's own scope, and it adds MCP resource governance plus preview session-policy endpoints. JumpCloud approaches the same gap from identity, issuing Agent Identities to non-human agents and fronting them with an AI Gateway, so an agent stops being an anonymous holder of a human's token.

ConductorOne · JumpCloud

PROTECT

Rank vulnerabilities by whether the code actually runs

Socket extends reachability to PHP/Composer and adds JS/TS workspace grouping and dynamic dispatch approximation, so a monorepo's alerts land on the package that really reaches the vulnerable call; a new `withheldFixes` field surfaces upgrades policy blocked, which otherwise disappear silently. cve-lite-cli splits findings prod-vs-dev in terminal and HTML output, killing the usual argument over a critical in a test harness.

Socket · cve-lite-cli

Does **Opus 5** read better? 👍 👎

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

Keygraph shannon

Feedback ⓘ 1 RELEASE · 2026-09-08 NOTES ↗

RANK

Shannon is an AI pentester for web applications and APIs. It analyzes your source code, identifies attack vectors, and executes real exploits to prove vulnerabilities before they reach production.

> Shannon v3.2.0 adds support for custom pi model configurations and improves visibility into startup and preflight errors.

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

01 **Custom pi model configs with registry-resolvable IDs** NEW

47

Shannon now supports custom pi model configs with registry-resolvable model IDs, and introduces distinct model error codes to help diagnose configuration issues.

— Names model config concept but no exact flag or file shown v3.2.0

02 **Startup and preflight failure visibility** IMPROVED

31

Shannon now surfaces startup and preflight failures so misconfiguration errors are visible before a scan begins, rather than failing silently mid-run.

— Describes behavior but no specific error format or command v3.2.0

WAS THIS USEFUL? 👍 👎

◆ Exploitation & C2

adscan

Feedback ⓘ 1 RELEASE · 2026-09-08 NOTES ↗ RANK

Free Active Directory pentesting tool for Linux. Automates AD and LDAP enumeration, Kerberoasting, ASREPRoast, password spraying, ADCS/ESC1, DCSync, RBCD, gMSA, shadow credentials, NTLM relay and credential dumping across 104 techniques, mapping BloodHound-compatible attack paths to Domain Admin.

> ADscan v12.0.0 ships native Windows support that removes the Docker/Python/nmap/Npcap dependency chain, alongside in-process port scanning, a CPU cracking fallback, smarter attack-path discovery for large directories, and massdns-free DNS resolution.

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

01 In-process Windows port scanning NEW

90

Adds in-process async TCP connect port scanning on Windows, replacing the nmap/Npcap dependency that hardened Windows hosts cannot satisfy. Throughput is tunable via the new `ADSCAN_PORTSCAN_CONCURRENCY` and `ADSCAN_PORTSCAN_PER_HOST` environment variables.

Raise port-scan throughput on a Windows host when you own the network and want faster coverage than the conservative default pacing.

```
$ set ADSCAN_PORTSCAN_CONCURRENCY=500 && set
ADSCAN_PORTSCAN_PER_HOST=20 && adscan.exe ci auth --type audit -
-interface Ethernet --domain corp.local --dc-ip 10.0.0.1 -u
alice -p 'S3cr3t!'
```

— Named env vars plus a runnable command v12.0.0

02 Native Windows support NEW

85

ADscan now runs natively on Windows as a self-contained bundle — no Docker, no Python, no nmap, no Npcap required — allowing a low-privilege user on a domain-joined Windows host to run a full scan.

Run a full authenticated scan from a domain-joined Windows host without Docker, Python, or nmap — common in assumed-breach engagements where you only have a locked-down Windows box.

```
$ adscan.exe ci auth --type audit --interface Ethernet --domain
corp.local --dc-ip 10.0.0.1 -u alice -p 'S3cr3t!'
```

— Names the exact command and dependencies removed v12.0.0

03 **Attack-path discovery scaling for large AD environments**

IMPROVED 75

Domain-wide attack-path discovery now targets Tier-0 (high-value) assets only, with the CLI printing an honest note listing those targets instead of silently launching an all-objects sweep. Discovery switches to a bounded per-target search when full analysis would exhaust available resources, covering every reachable high-value target on very large, dense directories. Reports and the web platform now plainly declare when attack-path routes are a representative sample rather than the full set, and surface a stable `exposure count` metric for tracking over time.

— Explains behavior and before/after but no exact command v12.0.0

THINNER COVERAGE BELOW

04 **CPU fallback for password cracking** NEW 55

Adds CPU fallback for password cracking of AS-REP and Kerberoast hashes on Windows hosts with no OpenCL/CUDA runtime, with recovered credentials recorded the same way as GPU cracks.

— Explains mechanism but no command shown v12.0.0

05 **Bulk DNS resolution without massdns** IMPROVED 50

Bulk DNS resolution no longer requires the external `massdns` binary, now resolving names concurrently through the DC — enabling host resolution on native Windows installs where `massdns` was unavailable.

— Names the removed dependency but no usage example v12.0.0

WAS THIS USEFUL? 👍 👎

BC Security Starkiller

Feedback ⓘ 1 RELEASE · 2026-09-08

NOTES ↗ RANK

Starkiller is a Frontend for Empire.

> Starkiller v4.0.3 introduces a Dashboard with an interactive agent topology graph, multi-tab terminal sessions, a per-agent stats view, and a revamped tag picker, alongside several module-execution refinements, Markdown-enabled chat, and a switch from yarn to pnpm for package management.

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

01 **Dashboard overview and topology graph** NEW 75

Adds a Dashboard overview page with summary metrics, agent check-ins, a recent-tasks list, an agents breakdown chart, and an interactive topology panel. The topology graph panel supports fullscreen expand and a context-aware right-click menu (Open, Popout, Execute shell/module, Kill, Focus), gains multi-agent selection on the Check Ins card, and both Dashboard and Graph View are now available to all users (previously restricted).

Visualize pivot chains across your active agents and launch actions without leaving the graph view.

> 📍 In the Dashboard, click the topology panel to open the interactive agent graph. Right-click any agent node to access the context menu: Open, Popout, Execute shell/module, Kill, or Focus. Use the fullscreen expand button (top-right of the panel) for a full-page view.

— Names UI elements and menu actions but no config/API surface v4.0.3

02 **Markdown rendering in chat** IMPROVED 75

Chat messages now render Markdown — bold, italic, strikethrough, inline code, code blocks, links, lists, blockquotes, and tables; links are hardened with `noopener` / `noreferrer` / `no-referrer` and restricted to `http` / `https`; the message box is now multi-line (Enter sends, Shift+Enter adds a newline).

— Enumerates every markdown feature and link-hardening attributes verbatim v4.0.3

03 **Package manager migration from yarn to pnpm** BREAKING

70

Package manager switched from yarn to pnpm 11, which requires Node 22+. Existing yarn-based installs must migrate to pnpm 11 before upgrading.

— States exact tool versions and required migration action v4.0.3

04 **Per-agent Stats tab** NEW

60

Adds a per-agent Stats tab on the agent page showing task counts, host info, and check-in and tasks-over-time charts.

Review task throughput and check-in cadence for a single agent without pivoting to the global dashboard.

> 📍 Navigate to Agents › select an agent › Stats tab to view task counts, host info, and check-in and tasks-over-time charts.

— Includes exact navigation path to reach the new tab v4.0.3

05 **Revamped v2 tag picker** IMPROVED

60

Adds a revamped v2 tag picker dialog for attaching tags to agents, listeners, and other taggable entities, featuring a filter box, a checklist of existing tags, and inline create-and-attach.

Organize agents by campaign or target using the new tag picker without leaving the agent view.

> 📍 Navigate to Agents › select an agent › Tags › open the tag picker dialog, type a tag name in the filter box to find or create it, then check it to attach it to the agent.

— Names UI mechanism and includes a usage path v4.0.3

06 **Module execution enhancements** IMPROVED

60

Adds a Background override toggle to module execution, auto-selects the best `DotNetVersion` based on the agent's installed .NET, renders Empire 7.0 typed boolean module options as toggle switches via the `value_type` option metadata, and filters the bypass picker to stagers matching the selected execution language.

— Names concrete metadata key and behaviors but no command example v4.0.3

THINNER COVERAGE BELOW

07 **Multi-tab terminal and shell sessions** NEW

45

Adds a dedicated Shell session tab and multi-tab Terminal support, with the terminal's live output buffer capped at 500 lines to bound memory growth on long-running

sessions.

— Describes the feature with a concrete limit but no navigation example v4.0.3

---

08 **Task stop confirmation prompt** NEW 20

Adds a confirmation prompt before stopping a running task.

— Single-line description with no mechanism detail v4.0.3

└──▷ **BREAKING ON UPGRADE**

! Package manager switched from yarn to pnpm 11, which requires Node 22+. Existing yarn-based installs must migrate to pnpm 11 before upgrading.

WAS THIS USEFUL? 👍 👎

◆ Post-Exploitation

SpecterOps BloodHound

Feedback ⓘ 1 RELEASE · 2026-09-08

NOTES ↗ RANK

Six Degrees of Domain Admin

> BloodHound's latest window centers on multi-destination pathfinding with drag-and-drop waypoint ordering, alongside a wave of smaller additions spanning artifact downloads, webhooks testing, notifications, and Posture Zone rule support.

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

01 Multi-destination pathfinding with waypoint reordering NEW

74

Adds an Add Destination control in the pathfinding UI that lets you route attack paths through up to two additional intermediate waypoint nodes in a user-specified traversal order; the Explore graph adds drag-and-drop reordering of these destinations.

When you need to trace a constrained attack path through a specific intermediate host or group before reaching the final target.

> 📍 In the BloodHound pathfinding view, set your source and target nodes, then select Add Destination to insert up to two intermediate waypoint nodes in the order you want BloodHound to traverse them.

– Names exact UI control and mechanism, includes usage steps v9.7.0

THINNER COVERAGE BELOW

02 Artifact download and lifecycle management NEW

48

Implements presigned artifact downloads, adds a support bundle download URL client method, and adds artifact expiration cleanup safeguards.

– Names three related additions but no config or command v9.7.0

03 Query parameter logging for /api/v2 requests NEW

45

Adds query parameter logging for `/api/v2` requests to improve auditability of API calls.

– Names endpoint path but no usage detail v9.7.0

04 JS client support for Zone Protected Asset score endpoint

IMPROVED

41

Updates the JS client to support the Zone Protected Asset score endpoint.

– Names endpoint but not method/path or usage v9.7.0

05 **Posture Zone rules via OpenGraph extension management** NEW 38

Adds database support for creating Posture Zone rules via OpenGraph extension management.

– Names feature area but no usage path or API v9.7.0

06 **Entity Panel templating support** NEW 38

Adds Entity Panel templating support along with `KindInfo` Markdown template validation.

– Names validation surface but no usage example v9.7.0

07 **Webhooks run-test dialog** NEW 37

Adds a webhooks run test dialog for validating webhook configurations.

– Names UI feature but no navigation path given v9.7.0

08 **Notifications and event history UI** NEW 33

Wires up notifications and event history tables in the UI and adds snackbar alerts for in-app notifications.

– Describes UI additions without mechanism or location v9.7.0

09 **Attack path selector in findings table** NEW 30

Adds an attack path selector to the findings table.

– Bare name, no mechanism or navigation detail v9.7.0

10 **New UI icons added** NEW 30

Adds `LinesWithMagnifyingGlass` icon and Floating Action Bar copy button icons to the UI icon set.

– Names specific icon but purely cosmetic addition v9.7.0

11 **Cypher query error metrics tracking** NEW 23

Tracks Cypher query error metrics.

– Bare mention, no metric names or access method v9.7.0

12 **Conditional default admin account in harness** NEW 23

Conditionally creates a default admin account in the harness.

– Internal harness change, minimal detail v9.7.0

13 **Keyboard navigation in UI** NEW

18

Adds keyboard navigation functionality to the UI.

— Bare mention with no scope or keys described v9.7.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

ZeroPath

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

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

> ZeroPath's biggest release yet ships a remote MCP server, Continuous Scanning across GitHub, GitLab, and both Bitbucket flavors, and new Gerrit and CVS source-control integrations, alongside Assistant skills, tighter permission controls, and a long tail of reporting, export, and UI improvements.

└──▷ WHAT SHIPPED · 27 FEATURES most completely described first ? what's the number?

01 Remote MCP server with audit-logged tool calls NEW

80

ZeroPath adds a remote MCP server at `https://zeropath.com/mcp` supporting Streamable HTTP clients (Claude, Cursor, Codex); connections are read-only until changes are approved, and administrators can revoke all org connections at once. Every MCP tool call is recorded to the audit log by parameter name, while credentials passed to a tool are never stored in audit rows or forwarded to a SIEM.

Connect Claude Desktop or Cursor to your ZeroPath findings with no API key — just point the client at the hosted MCP server and authenticate via browser.

```
$ https://zeropath.com/mcp
```

— Endpoint and clients named; connection steps not fully detailed.

changelog-20260909-ed06a3ad

02 Microsoft Teams alerts via incoming webhook NEW

80

ZeroPath adds Microsoft Teams channel notifications via an incoming webhook — paste the webhook URL into ZeroPath to deliver scan notifications and vulnerability alerts as Adaptive Cards, with no Azure AD app registration required.

Route ZeroPath scan notifications to a Microsoft Teams channel without Azure AD — create an incoming webhook in Teams and register it in ZeroPath.

📍 In ZeroPath, go to Settings › Connections › Notifications, select Microsoft Teams, and paste the incoming webhook URL generated from your Teams channel settings.

— Exact setup steps and webhook path provided. changelog-20260909-ed06a3ad

03 **Continuous Scanning on every meaningful commit** NEW

80

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

— Behaviour and scope fully described; no exact toggle path given.

changelog-20260909-ed06a3ad

04 **New granular permissions for integrations, repositories, and tickets**

80

BREAKING

Connecting an integration now requires the Create Integrations or Create Installations permission; adding a repository by URL requires Create Repositories ; and creating Jira and Linear tickets now requires a per-repository permission. Existing automations lacking these grants will be refused, and organizations using access control must explicitly grant the ticketing permission or ticket creation will be unavailable.

— Exact permission names given; migration action is clear. changelog-20260909-ed06a3ad

05 **`lastScanFailure` field replaces `lastScanError`** BREAKING

75

The repository object's `lastScanError` field is replaced by `lastScanFailure`, which carries both the message and the outcome of a failed scan. API clients or integrations still reading `lastScanError` will receive no value.

— Exact field names given; no migration guidance beyond rename.

changelog-20260909-ed06a3ad

06 **Assistant skills for reusable methodologies** NEW

75

Assistant skills are reusable methodology definitions authored from the Skills tab, with four built-in skills for triage, dependency reachability, report writing, and patch review — each forkable into an editable copy.

— Names Skills tab and four built-ins; no API or flag given. changelog-20260909-ed06a3ad

07 **Pull request submission status and retries** NEW

75

Approved patches now show pull request submission status — queued, in progress, waiting on retry, or stopped — with Cancel and Retry actions on the issue itself, and up to five automatic submission attempts.

— States exact statuses and retry limit; UI path implicit only.

changelog-20260909-ed06a3ad

08 **CVS module support** NEW 65

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

— Protocols and scan types named; no exact command shown. changelog-20260909-ed06a3ad

09 **Team import from GitHub and Bitbucket** NEW 65

ZeroPath adds team import from GitHub and Bitbucket — covering Bitbucket Cloud workspace groups and Bitbucket Server project groups — to sync repository permissions and access control.

— Named sources given; no exact import steps. changelog-20260909-ed06a3ad

10 **CVSS-banded severity labels** NEW 65

ZeroPath adds severity labels following CVSS rating bands — Critical (9.0+), High (7.0+), Medium (4.0+), Low (0.1+) — applied to existing findings without requiring a rescan.

— Exact band thresholds given; no config surface named. changelog-20260909-ed06a3ad

11 **Scope filtering for reports and Supply Chain** NEW 65

ZeroPath adds an optional tag and repository scope parameter to monthly, organization summary, SLA compliance, and SOC 2 reports, stated on the report cover, and a separate scope control at the top of Supply Chain that narrows every tab to a selected set of repositories, teams, and tags.

— Names all report types and Supply Chain scope; no exact UI steps.

changelog-20260909-ed06a3ad

12 **Reorganized Settings navigation and scanner scopes** IMPROVED 65

Settings now has grouped navigation with Workspace, Security, and Connections sidebar sections; scanner settings expose the same five categories — General, Full scans, Pull requests, Dependencies, Remediation — at organization, tag, and repository scope.

— Names all sections and scopes; no direct navigation link. changelog-20260909-ed06a3ad

13 **Gerrit project support** NEW 60

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

— Mechanism described but no config or flag names given. changelog-20260909-ed06a3ad

14 **'Plan first' mode in Assistant** NEW 60

The Assistant gains a Plan first mode: it proposes an editable plan before execution and offers to save the approved plan as a schedule, trigger, or playbook.

— Workflow described; no UI path or command given. changelog-20260909-ed06a3ad

15 **Wiz export for dependency findings** NEW 60

ZeroPath adds Wiz export support that marks already-resolved dependency findings as resolved in Wiz and sends unassessed findings as new records.

— Behaviour described; no endpoint or config key given. changelog-20260909-ed06a3ad

16 **Secret dismissal explanations withheld from API** BREAKING 60

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

— Exact behaviour change stated; no migration path given. changelog-20260909-ed06a3ad

THINNER COVERAGE BELOW

17 **Dependency findings tab on Issues page** NEW 55

ZeroPath adds a dependency findings tab to the Issues page with CVE, advisory, and package search.

— Names tab location and search fields; no query syntax. changelog-20260909-ed06a3ad

18 **Expanded language coverage for repository sizing** NEW 55

ZeroPath adds Terraform, Svelte, Vue, Solidity, Elixir, Dart, protobuf, and Genero to repository size calculations, ensuring those repositories receive the analysis depth their size warrants.

— Lists all languages; sizing mechanism itself not detailed. changelog-20260909-ed06a3ad

19 **Secrets scanning coverage reporting** NEW 55

ZeroPath now reports secrets scanning coverage: it states the coverage achieved and names any file too large to read within the scan's time budget.

— Explains what's reported; no config or threshold given. changelog-20260909-ed06a3ad

20 **CVSS v4.0 vector support** NEW 50

ZeroPath adds CVSS v4.0 vector support, assessing subsequent-system impact on its own evidence.

— Mechanism named briefly; no scoring detail or UI location. changelog-20260909-ed06a3ad

21 **On-demand Jira ticket sync preview** NEW 50

ZeroPath adds an on-demand Jira ticket sync preview that shows what each linked ticket will do before you apply it.

— Describes preview behaviour; no exact endpoint or UI path. changelog-20260909-ed06a3ad

22 **Jira and Linear ticket links in exports** NEW 50

ZeroPath adds Jira and Linear ticket links to CSV exports and the export endpoint.

— Names export surfaces; no endpoint path given. changelog-20260909-ed06a3ad

23 **'Needs Review' queue state for unassessed findings** NEW 45

ZeroPath adds a Needs Review queue state for findings it has not yet assessed, ranking them on severity alone.

— Describes state and ranking; no filter or API name. changelog-20260909-ed06a3ad

24 **GitHub Enterprise Cloud with data residency** NEW 35

ZeroPath adds GitHub Enterprise Cloud with data residency as a supported version control connection.

— Named integration only; no setup detail given. changelog-20260909-ed06a3ad

25 **'What's new' release panel** NEW 35

A What's new panel in the top bar shows the three most recent releases, marking unread ones.

— Simple UI addition, no further mechanism. changelog-20260909-ed06a3ad

26 **Pull request address added to scan webhooks** NEW 35

ZeroPath adds pull request address to pull request scan webhooks.

— Single field addition with no payload schema shown. changelog-20260909-ed06a3ad

27 **Full-year dashboard view with quarterly option** IMPROVED 35

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

— Brief UI change with minimal detail. changelog-20260909-ed06a3ad

╰──▷ BREAKING ON UPGRADE

! On the repository object, `lastScanError` is replaced by `lastScanFailure`; any API client or integration reading `lastScanError` will receive no value.

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

lacking these grants will be refused.

! Creating Jira and Linear tickets is now a per-repository permission; organizations using access control must explicitly grant it or ticket creation will be unavailable.

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

WAS THIS USEFUL?  

Aikido Security

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

RANK

Aikido Security is a developer-focused security platform that scans code and infrastructure for vulnerabilities and misconfigurations.

> Aikido's biggest release this window adds Code Coverage for GitHub, 11 SIEM integrations for issue correlation, and Pentest for AI Capabilities covering the OWASP Agentic Top 10, alongside new API endpoints, Terraform provider resources, a Device Protection firewall, and Deep Review billing limits with GitLab support.

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

01 **PR check management via Terraform and API** NEW 75

Aikido adds `new resource to manage default PR checks` and `new resource to manage PR check settings` to the Aikido Terraform provider, alongside the `API - Manage defaults PR checks for new repos` endpoint to control default PR check configuration for new repos programmatically.

— Names exact Terraform resources and API endpoint, but no usage example.

#55 - Code Coverage for Github, SIEM In…

02 **New API endpoints for compliance export and inbox management** NEW 60

Aikido adds the `API - Report export for PCI and DORA compliance` endpoint to export compliance reports programmatically, and the `API - Listing & handling inbox requests` endpoint to manage inbox requests via the API.

— Endpoints named verbatim but no method, params or example calls.

#55 - Code Coverage for Github, SIEM In…

THINNER COVERAGE BELOW

03 **Pentest for AI capabilities** NEW 55

Aikido adds Pentest for AI Capabilities targeting the OWASP Agentic Top 10 (including prompt injection and memory poisoning) for AI agents and LLM features.

— Named framework and threat types but no how-to or scope details.

#55 - Code Coverage for Github, SIEM In…

04 **Code Coverage for GitHub** NEW 50

Aikido adds Code Coverage for GitHub to surface which parts of a codebase ship with zero tests, with one-step setup and no secrets to manage.

— Explains purpose and setup ease but no exact steps or UI path.

#55 - Code Coverage for Github, SIEM In…

05 **SIEM integrations for issue forwarding** NEW 40

Aikido adds SIEM integrations supporting 11 SIEMs, enabling Aikido issues to be forwarded and correlated with other organizational security data.

— Count of SIEMs given but none named individually.

#55 - Code Coverage for Github, SIEM In…

06 **Deep Review billing limits and GitLab support** IMPROVED 35

Aikido adds monthly billing limits and GitLab support to Deep Review.

— Two named additions but no mechanism or limit values given.

#55 - Code Coverage for Github, SIEM In…

07 **Firewall for Device Protection** NEW 30

Aikido adds a new Firewall to Device Protection to block malicious domains.

— Bare description of function with no configuration detail.

#55 - Code Coverage for Github, SIEM In…

WAS THIS USEFUL? 👍 👎

OX Security

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

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

> OX Security added Dependency Vetting to OX VibeSec, which inspects every package an AI coding agent attempts to install and blocks known-malicious or brand-new packages before they reach a developer machine or SBOM.

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

01 **Dependency Vetting for AI agent installs** NEW 53

OX VibeSec now inspects every AI agent install attempt against policy, blocking known-malicious packages outright before they touch the developer machine or the SBOM. It also introduces a configurable cool-down period that blocks freshly published packages until the community has had time to flag them.

— Describes mechanism and scope but no exact config key or command shown.

Vet Every Dependency Your Agents Instal…

WAS THIS USEFUL? 👍 👎

GitHub

Feedback ⓘ 5 RELEASES · 2026-09-08 → 2026-09-09 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 headline ship this window is agentic autofix for Code Quality findings, alongside GitHub Enterprise Server 3.22 reaching general availability with enterprise teams, ruleset bypass-by-user, and required-reviewer rules. It also shipped enterprise-managed sandbox policies and IDE-aware CLI integration for Copilot in JetBrains, a unified `help.github.com` customer portal, and automatic Dependabot access to private GitHub Packages registries.

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

01 Automatic Dependabot access to GitHub-hosted registries

IMPROVED 95

Dependabot's `GITHUB_TOKEN` now automatically requests the `packages: read` permission and sends that token when pulling from `*.pkg.github.com` and `ghcr.io`, removing the need for PAT-based registry entries in `dependabot.yml`. Dependabot reuses existing Manage Actions access grants on package settings pages to authenticate with private GitHub Packages registries, covering every GitHub Packages ecosystem Dependabot supports.

Grant Dependabot read access to a private GitHub Package so it can resolve updates without a PAT — replaces any PAT-based registry block you previously added to dependabot.yml.

📍 1. Go to your organization's or personal account's Packages tab and open the target package. 2. Under Manage Actions access, click Add repository. 3. Select the repository that runs Dependabot and set access to Read. 4. Remove the corresponding PAT-based entry from dependabot.yml (no other changes needed).

— Names token, permission, hosts, config file, and exact steps

Automatic Dependabot access to GitHub-h…

02 Agentic autofix for Code Quality findings NEW 85

A new Assign to Copilot bulk action lets you select up to 25 standard Code Quality findings and have Copilot fix them agentically on a branch, validate its own changes, and open a pull request for review. Available for repositories with GitHub Code Quality enabled on GitHub Team and GitHub Enterprise Cloud, including data residency, governed by the existing enterprise GitHub Code Quality policy with no separate policy to manage.

Burn down a backlog of code quality findings by assigning a batch to Copilot, which opens a PR with validated fixes for each one.

> 📍 In your repository, go to Code Quality › Findings. Select up to 25 standard findings using the checkboxes, then choose `Assign to Copilot` from the bulk-action menu. Copilot will fix them on a new branch and open a pull request for your review.

— Names the bulk action, limit, and exact UI path

Remediate Code Quality findings with ag…

03 **Required reviewers rule for rulesets** NEW 80

A new required reviewers rule for repository rulesets supports pattern matching on branches, files, and folders, and a configurable minimum number of reviews per team.

Require the security team to review all changes to the default branch by adding a required reviewers rule to a repository ruleset — enforcing sign-off from teams beyond CODEOWNERS.

> 📍 In your repository, go to Settings › Rules › Rulesets › New ruleset, set the target branch to `main`, add a `Required reviewers` rule, select your security team, and set the minimum number of required reviews.

— Names matching scope and gives exact setup steps

GitHub Enterprise Server 3.22 is now ge…

04 **Enterprise-managed sandbox policies for Copilot JetBrains** NEW 78

Administrators can centrally control sandbox enablement, filesystem and network access, proxy settings, developer-tool access, and macOS Keychain access via managed restrictions that override user settings. Visible under `GitHub Copilot > Sandbox` when the Editor Preview feature flag is on or a managed setting is configured; currently in public preview.

— Names exact settings path and override scope Enterprise-managed sandbox in Copilot f…

05 **/ide command in Copilot CLI** NEW 75

The new `/ide` command in GitHub Copilot CLI (public preview) connects a terminal session to JetBrains IDE context, including selections, diagnostics, and file references. Shell commands can consume IDE terminal environment variables and the project's configured Python interpreter, and can activate the project's local Python virtual environment.

— Names the command and what context it exposes Enterprise-managed sandbox in Copilot f…

06 **Ruleset bypass by individual users** NEW 70

Repository rulesets now support bypass by individual users, allowing administrators to add specific accounts, such as a service account, to a bypass list without creating a dedicated role or team.

Grant a service account ruleset bypass rights without creating a dedicated role or team — useful for automated merge workflows in CI/CD.

> 📍 In your repository, go to Settings › Rules › Rulesets, open the target ruleset, navigate to Bypass list, click `Add bypass`, search for the service account by username, and save.

— Exact UI path to grant bypass is given `GitHub Enterprise Server 3.22 is now ge…`

---

07 **Unified customer portal at help.github.com** NEW 60

A new unified portal at `help.github.com` consolidates support, entitlements, docs, learning, community, and account resources into a single entry point, with Copilot-powered search across all portal content available without sign-in, and product status and announcements surfaced directly within the portal.

— Names the domain and consolidated content areas

`New customer portal help.github.com (20…`

THINNER COVERAGE BELOW

08 **Air-gapped Copilot CLI support for GHES** NEW 55

GHES can now be configured to work with Copilot CLI in disconnected or air-gapped environments: administrators set up a model provider once in GHES and end users authenticate with their GHES credentials. Currently a technical preview.

— Explains setup model but no configuration steps

`GitHub Enterprise Server 3.22 is now ge…`

09 **Copilot for JetBrains editor, chat and diagnostics enhancements**

NEW

50

Adds cross-file cursor jumps in next edit suggestions so Copilot can move the cursor to the relevant location in another file; adds global project context in chat so global files/folders persist across a project instead of being re-added per session; adds enterprise policy diagnostics to verify Copilot policies are correctly detected and enforced on a device; adds support for selecting the session model used by built-in subagents in the Copilot agent harness; and promotes OpenTelemetry settings in GitHub Copilot – Chat to general availability for all users.

— Five thin additions named but no mechanism or steps

Enterprise-managed sandbox in Copilot f…

10 **Enterprise teams general availability** IMPROVED

45

Enterprise teams reach general availability, letting enterprise owners manage users and access across all organizations and repositories from a single centralized team structure.

— States benefit and GA status but no mechanism detail

GitHub Enterprise Server 3.22 is now ge…

11 **Sort secret scanning bypass and dismissal requests by date**

IMPROVED

40

Secret scanning push protection bypass requests and alert dismissal requests can now be sorted by date, ascending or descending, via the filter bar at repository, organization, and enterprise levels.

— Names the filter bar but no example given GitHub Enterprise Server 3.22 is now ge…

12 **Release badge in issue sidebar** NEW

30

The issue sidebar now displays a Latest release or Pre-release badge when a linked pull request has been included in a release.

— One-line UI addition, no further detail GitHub Enterprise Server 3.22 is now ge…

13 **Contributor role labels in pull request list** NEW

30

The pull request list view for public repositories now shows contributor role labels: First-time contributor, Contributor, Member.

— One-line UI addition, no further detail GitHub Enterprise Server 3.22 is now ge…

WAS THIS USEFUL? 👍 👎

GitLab

Feedback ⓘ 2 RELEASES · 2026-09-08 BLOG ↗ RANK

The intelligent orchestration platform for DevSecOps, enabling teams and agents to ship trusted software at enterprise scale.

> GitLab's biggest AI move this window is opening GitLab Duo Self-Hosted to Microsoft Foundry-hosted models with per-feature assignment, alongside a new faster GPT-6 Astra option on Duo Agent Platform and a CI include-resolution fix.

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

01 Microsoft Foundry backend for GitLab Duo Self-Hosted NEW

88

GitLab Duo Self-Hosted can now register model deployments on Microsoft Foundry using the `azure/<deployment-name>` model identifier format, supporting GPT, Claude, Llama, and Mistral families served through Azure-hosted endpoints via the AI Gateway. Per-feature model assignment lets admins assign a different deployment (e.g. `duo-chat`, `duo-code-gen`, `duo-code-completion`) to each Duo feature instead of one global model, and Foundry deployments support Microsoft Entra identity, Azure RBAC, network isolation, and Azure Policy while keeping inference data inside the organization's own Azure tenant.

Register a Microsoft Foundry model deployment for GitLab Duo Agentic Chat, pointing GitLab at the Foundry endpoint with the `azure/` identifier prefix.

> 📍 Admin › GitLab Duo › Configure models for GitLab Duo › Add self-hosted model Deployment name: Agentic Chat on Microsoft Foundry Model family: GPT Endpoint: https://<your-foundry-endpoint>.`openai.azure.com` / API key: <your-api-key> Model identifier: azure/duo-chat

Point the GitLab instance at a locally running AI Gateway so that self-hosted model requests are routed through infrastructure you control.

> 📍 Admin › GitLab Duo › Change configuration Local AI Gateway URL: `https://ai-gateway.example.com:5052` Select Save changes

— Names identifier format, per-feature keys, and exact admin steps

Bring your own model to GitLab Duo Self…

02 CI include resolution uses declaring file's context NEW

65

New `ci_spec_include_own_context` feature flag (GitLab 19.4) makes `include` locations in a CI config file resolve against the repository and ref of the file that declares them, rather than the file that included them.

— Names exact flag and version but no usage example product docs

THINNER COVERAGE BELOW

03 **GPT-6 Astra model on Duo Agent Platform** NEW 46

GPT-6 Astra is now selectable on GitLab Duo Agent Platform, with admins able to assign it per feature via model selection settings; it runs 43% faster and uses 43% fewer tokens than GPT-5.6 Sol.

— Gives concrete performance numbers but no config or steps

GPT-6 Astra on GitLab: Faster runs, few…

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ 3 RELEASES · 2026-09-08 → 2026-09-09 BLOG ↗

RANK

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

> Veracode expanded its AI-assisted Fix remediation to cover SAST and SCA across IDEs, the CLI, SCM integrations, and GitHub Workflow Integration, while overhauling Security Labs training with platform-integrated administration, a full OWASP Top 10:2025 course and lab refresh, and deprecation of older OWASP-aligned content; it also shipped smaller integration updates for Azure DevOps, the Java API Wrapper, and GitHub/VS Code tooling.

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

01 Fix for SCA across CLI, SCM, and GitHub NEW

95

Fix for SCA analyzes vulnerable dependencies identified in SCA scans and suggests safe upgrade paths. The `veracode fix sca` CLI command (Limited Availability) generates remediation patches; running Fix for SCA via the CLI requires the `--remote` flag, which executes in a backend sandbox with full source access for automated CI pipelines, scheduled jobs, and SCM workflows. SCM integration (Fix in SCM) scans a repository, generates patches, and opens merge requests automatically, and GitHub Workflow Integration now also supports Fix for SCA, generating fixes for vulnerable dependencies directly in GitHub.

Run Fix for SCA in a CI pipeline, where the remote backend sandbox handles transitive dependencies and batches findings comprehensively.

```
$ veracode fix --remote
```

Automatically generate a remediation patch for a vulnerable dependency identified in an SCA scan, so you can apply a safe upgrade without manually researching fix paths.

```
$ veracode fix sca
```

— Runnable CLI commands and flag named for immediate use Fix updates (2026-09-08) Integration updates (2026-09-08)

02 Azure DevOps Workflow Integration configuration options NEW

85

Azure DevOps Workflow Integration v2.4.3 adds a custom agent pool name parameter in `veracode.yml` to specify the agent pool used for pipeline execution. The `veracode.yml` config also supports `debug: true` for verbose troubleshooting output and `analysis_branch` to run scheduled scans against a specific branch rather than the repository default.

Enable verbose debug output in an Azure DevOps Workflow Integration pipeline to troubleshoot scan failures.

```yaml
debug: true
```

Run scheduled Azure DevOps scans against a specific analysis branch rather than the repository default branch.

```yaml
analysis_branch: main-security-scan
```

— Exact config keys with runnable example values Integration updates (2026-09-08)

03 **Get Lesson Progress API enhancements** IMPROVED 75

The Get Lesson Progress API adds an `updatedAfter` parameter to support incremental data loads and an `excludeNotStarted=true` parameter to filter out lessons that have not been started. The response now includes `stack` and `updated_on` fields, and surfaces a Not Started status when both `start_time` and `end_time` are null.

— Exact API parameters and fields named but no endpoint path given

Training updates (2026-09-09)

04 **New OWASP-aligned training content and labs** NEW 75

Adds six new OWASP Top 10:2025 secure coding eLearning courses covering .NET, Java, JavaScript, PHP, Python, and general software security awareness, with captions in English, Spanish, French, Portuguese, and Chinese. Adds the complete OWASP Top 10:2025 Security Labs lab series (A01–A10), including two new categories, A03 Software Supply Chain Failures and A10 Mishandling of Exceptional Conditions. Adds a Container Security in Docker Security Labs lesson track spanning Capabilities, Users, Virtualization, Networking, Resources, Orchestration, and Inventory topics. Adds OWASP API Top 10 2023 Security Labs lessons, upgrading coverage from the 2019 list and adding three new categories (API 6, API 7, API 10) in Java, Node, and .NET. Adds five assessment quiz eLearning courses (User and application setup, Static Analysis, Dynamic Analysis, Scan and fix in your IDE, SCA agent-based scanning — Skills assessment) in English, Portuguese, and Spanish.

— Every course and lab category named, but no direct link given

Training updates (2026-09-09)

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

The default Security Labs URL has changed from `https://securitylabs.veracode.com/` to `https://securitylabs.veracode.com/security-labs/`; organizations using SSO with the old URL must update their SSO configuration.

— Exact old and new URLs with required migration action Training updates (2026-09-09)

06 **GitHub Workflow Integration platform-managed lifecycle** NEW 70

GitHub Workflow Integration v2.0.0 enables install, configuration, and credential updates for the GitHub Integration directly from the Veracode Platform, eliminating manual GitHub Marketplace steps; adds autopackaging support for Apex, VB6, and Perl; and adds the ability to schedule Static Analysis, SCA, and IaC scans for GitHub organizations directly from the Platform. v2.1.1 adds a new uninstallation workflow on the Platform for removing the Veracode app from GitHub organizations.

— Version numbers and scope named but no config/API detail

Integration updates (2026-09-08)

07 **Fix for SAST across IDEs and CLI** NEW 65

Fix for SAST provides interactive, in-editor remediation in Eclipse, JetBrains, Visual Studio, and VS Code IDEs, and via the Veracode CLI (`Fix in CLI`) for both interactive use and automated scripting in CI pipelines. COBOL is now supported, with automated fix suggestions for `CWE-78` , `CWE-209` , `CWE-248` , `CWE-489` , and `CWE-252` , available in the CLI and in Visual Studio Code, Visual Studio, and JetBrains IDEs.

— Names IDEs and CWEs but no exact CLI command shown `Fix updates (2026-09-08)`

08 **Applications API retry mechanism** IMPROVED 65

Java API Wrapper v26.2.18.0 implements a configurable retry mechanism for the Veracode Platform Applications API (`appsec/v1/applications`) to handle transient failures, timeouts, and network issues.

— Named endpoint and version but no retry parameters given

`Integration updates (2026-09-08)`

09 **Deprecated OWASP training content** DEPRECATED 65

33 deprecated eLearning courses (OWASP 2017, OWASP Top 10 2021, Secure Coding for .NET/Java/JavaScript/PHP/Python — 6 courses each, Secure Coding for Python — 3 courses) are no longer available as of June 2026; certification levels have been updated to reference the replacement OWASP Top 10:2025 courses. OWASP Top 10 (2021) Security Labs lessons are also no longer available as of June 2026.

— Exact deprecated course list and removal date given `Training updates (2026-09-09)`

10 **Security Labs administration integrated into Veracode Platform** NEW 60

Security Labs user and team management is now integrated into the Veracode Platform, with authentication routed through Veracode IAM; administrators manage users and teams from the Platform under Security Training. Adds team search capability for Security Labs administrators and managers, and in-app guidance in Security Labs for creating campaigns and using reporting.

— Clear UI path but no config or API detail `Training updates (2026-09-09)`

THINNER COVERAGE BELOW

11 **Security Labs terminology rename** BREAKING 55

In Security Labs, `Teams` are renamed to `Organizations` and `Roles` are renamed to `Teams` ; any documentation, scripts, or integrations referencing these terms must be updated.

— Names the exact rename mapping but no further mechanism `Training updates (2026-09-09)`

12 **CWE tagging in Security Labs lessons** NEW 50

Adds CWE tagging to Security Labs lessons, enabling admins to search by CWE or title and learners to see CWE associations per lesson.

— Explains search and display behavior but no exact UI path Training updates (2026-09-09)

13 **VS Code extension installation and settings** NEW 40

The Veracode VS Code extension adds a guided installation flow and settings screens, including a general settings tab, a policy menu configuration screen, and a proxy configuration setting.

.
.
.
.

— Based only on screenshots, no accompanying text description

Integration updates (2026-09-08)

14 **eLearning date-range filter** NEW 30

Adds an eLearning date-range filter allowing report start dates up to one year in the past.

— Single thin line with no further mechanism Training updates (2026-09-09)

15 **Code syntax highlighting in Security Labs lessons** IMPROVED 30

Adds code syntax highlighting to Security Labs lessons, tailored to the programming language of each code sample.

— Single-line description with no further detail Training updates (2026-09-09)

└──▷ BREAKING ON UPGRADE

! The default Security Labs URL has changed from `https://securitylabs.veracode.com/` to `https://securitylabs.veracode.com/security-labs/` — organizations using SSO with the old URL must update their SSO configuration.

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

! 33 deprecated eLearning courses (OWASP 2017, OWASP Top 10 2021, Secure Coding for .NET/Java/JavaScript/PHP/Python — 6 courses each, Secure Coding for Python — 3 courses) are no longer available as of June 2026; certification levels have been updated to reference the replacement OWASP Top 10:2025 courses.

! OWASP Top 10 (2021) Security Labs lessons are no longer available as of June 2026.

WAS THIS USEFUL? 👍 👎

cve-lite-cli

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

Fast, developer-friendly JS/TS dependency vulnerability scanner with local lockfile scanning, OSV matching, direct vs transitive visibility, --fix, JSON output, and practical remediation guidance.

> cve-lite-cli added SBOM export in SPDX 2.3 and upgraded CycloneDX 1.6 formats, a new inventory-only SBOM mode, and a prod-vs-dev findings split in terminal and HTML reports.

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

01 **SPDX 2.3 SBOM export via --sbom flag** NEW 95

`--sbom spdx2.3` (also `--sbom spdx`) writes a timestamped `.spdx.json` SBOM in SPDX 2.3 format. Findings attach as `SECURITY` external references of type `advisory`, with severity and fix command recorded in a package annotation; package licenses are sourced from the npm lockfile at no network cost, while pnpm, Yarn and Bun dependencies resolve to `NOASSERTION`. The output emits `supplier`, `filesAnalyzed: false` and `DEPENDENCY_OF` relationships to satisfy all seven NTIA minimum elements.

Generate a full SPDX 2.3 SBOM with vulnerability overlays attached as SECURITY references — useful for NTIA-compliant software bills of materials in regulated environments.

```
$ cve-lite /path/to/project --sbom spdx2.3
```

Export an SPDX 2.3 SBOM with full vulnerability overlay after a scan — useful for feeding into a software supply-chain pipeline or compliance tooling.

```
$ cve-lite . --sbom spdx
```

Generate an SPDX 2.3 SBOM with vulnerability data included during a scan, for submission to a supply-chain compliance pipeline.

```
$ cve-lite . --sbom spdx
```

— Full mechanism, formats and flag named. v1.34.0

02 **CycloneDX SBOM output upgraded to spec 1.6** BREAKING 85

`--sbom cyclonedx` (alias for the existing `--cdx`) now emits CycloneDX spec version `1.6` instead of `1.4`, using the 1.6 `tools.components` object form with `publisher` in place of the deprecated 1.4 array of `{vendor, name, version}`. This is a breaking change: any CI pipeline or tooling that diffs SBOMs, asserts on `specVersion`, or parses `metadata.tools` will need updating.

Generate a pure component inventory (no vulnerability data) in CycloneDX format — useful when your SBOM consumer expects only a bill-of-materials without vuln annotations.

```
$ cve-lite . --sbom cyclonedx --sbom-inventory-only
```

— Names exact spec version, flags and breaking impact. v1.34.0

03 **SBOM inventory-only mode** NEW 75

`--sbom-inventory-only` emits an SBOM without the vulnerability overlay, producing a pure component inventory; it requires `--sbom` and is intended for diffing, archival and attestation workflows where finding details should not be exposed.

Produce a clean dependency inventory SBOM with no vulnerability data for diffing across CI runs or submitting for attestation without exposing finding details.

```
$ cve-lite /path/to/project --sbom spdx --sbom-inventory-only
```

Produce a clean software inventory (no vulnerability overlay) in CycloneDX format, suitable for sharing with a vendor or archiving as a build artifact.

```
$ cve-lite . --sbom cyclonedx --sbom-inventory-only
```

— Named flag with clear purpose and requirement. v1.34.0

THINNER COVERAGE BELOW

04 **Prod-vs-dev findings split in reports** IMPROVED 45

Compact and verbose terminal output, and the HTML report severity card strip, now show a 'N of M findings in prod dependencies' note whenever some findings are dev-only, across all report formats.

— Describes behavior but no flag or config named. v1.34.0

└──▷ BREAKING ON UPGRADE

! CycloneDX output (`--cdx` and `--sbom cyclonedx`) now emits `specVersion` `1.6` instead of `1.4`; any CI pipeline or tooling that diffs SBOMs or asserts on the `specVersion` field will need updating.

! `metadata.tools` in CycloneDX output now uses the 1.6 `tools.components` object form with `publisher`, replacing the deprecated 1.4 array of `{vendor, name, version}`; downstream consumers parsing `metadata.tools` will see a different structure.

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

GitGuardian Detection Engine

Feedback ⓘ

1 RELEASE · 2026-08-31 BLOG ↗ RANK

GitGuardian Detection Engine scans code repositories to identify and alert on exposed secrets, credentials, and sensitive data.

> GitGuardian's Detection Engine 2.171 release adds two new secret analyzers and sharpens detection accuracy across three existing analyzers.

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

01 **Detection accuracy improvements to existing analyzers** IMPROVED

60

The `generic_high_entropy_secret` detector no longer reports secrets whose assigned variable ends with `checksum`, with no loss of recall. The n8n MCP Access Token and n8n API Key detectors now recognize hosts given as a container service name or as a scheme-less hostname, and reject unreachable private IP hosts. Recall for HashiCorp Vault AppRole Authentication credentials was also improved.

— Names exact detectors and behavior changes but no metrics

Detection Engine Updates Version 2.171 …

THINNER COVERAGE BELOW

02 **New secret analyzers for Akamai and Docker Hub** NEW

30

Adds a secret analyzer for Akamai API Credentials and a new analyzer for Docker Hub personal access tokens.

— Names two new detectors but no mechanism given Detection Engine Updates Version 2.171 …

WAS THIS USEFUL? 👍 👎

◆ Digital Forensics & Incident Response

iLEAPP

Feedback ⓘ 1 RELEASE · 2026-09-08 NOTES ↗ CODE ↗ RANK

iOS Logs, Events, And Plist Parser

> iLEAPP v2026.3.3 adds MMKV decryption support, ingests iOS diagnostic reports and sysdiagnose extractions, and ships 25+ new app parsers alongside targeted fixes to SMS, TikTok, Line and Discord parsing.

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

01 **--emit flag for sample data generation** NEW 85

Adds `--emit` flag to `validate_sample_data.py` to generate `sample_data` values directly from a test extraction image, e.g. `python admin/scripts/validate_sample_data.py --emit extraction.zip --key my_test_image`.

Generate ready-to-paste `sample_data` blocks for all modules changed on your branch, using a full extraction as input.

```
$ python admin/scripts/validate_sample_data.py --emit
extraction.zip --key my_test_image
```

— Named flag plus a runnable command from the input. v2026.3.3

02 **MMKV decryption support and Recovered Records artifact** NEW 70

Adds MMKV decryption support via a vendored `mmkv_parser`, with correct varint header handling and a new MMKV - Recovered Records artifact.

— Names the parser, header handling and artifact but no CLI usage shown. v2026.3.3

03 **TikTok artifact container scoping** IMPROVED 65

Scopes TikTok IM, Pitaya, and WatchHistory artifacts to TikTok-owned containers, preventing false matches from files with identical names in other app containers.

— Explains the false-match problem and its fix in detail. v2026.3.3

04 **25+ new app parsers added** NEW 60

Adds 25+ new app parsers including Nest, August/Yale, Google Home, myQ, Samsung Family Hub, Coinbase Wallet, Spotify, TextNow, Zoom chat, Brave, Notion, GETTR, Houseparty, CoverMe, Skout, Private Photo Vault, IFTTT, LG ThinQ, New York Times, GPS Tracks/GPX, and Foursquare Pilgrim.

— Long named list but no detail on what each parser extracts. v2026.3.3

THINNER COVERAGE BELOW

05 **Expanded forensic input formats** NEW

55

Adds support for ingesting iOS diagnostic reports (`.ips` files) as a new input format, and adds a Sysdiagnose Extraction Helper to expand raw forensic input options.

— Names two new input surfaces but not how to invoke the helper. v2026.3.3

06 **New SMS artifact fields** IMPROVED

55

Adds Sender , Chat Name , and Chat Participants fields to the SMS artifact.

— Names exact fields added, no further mechanism given. v2026.3.3

07 **New artifacts across Life360, WhatsApp, Signal and Chromium logs**

NEW

50

Adds Life360 location samples and motion activity parsed from app logs, a WhatsApp log sessions artifact for iOS, Signal app launches and call events parsed from iOS debug logs, and Chromium tab restore file parsing on iOS.

— Names four new artifacts across apps but no extraction mechanism. v2026.3.3

08 **Line messenger multi-store database parsing** IMPROVED

50

Extends Line messenger to read every database store rather than only the first, and reports orphaned attachments.

— Describes the before/after change but no field or command names. v2026.3.3

09 **Discord account artifact reworked for MMKV store** IMPROVED

45

Reworks the Discord iOS account artifact to read account data directly from its MMKV store.

— States the before/after mechanism but no further detail. v2026.3.3

WAS THIS USEFUL? 👍 👎

UAC

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

UAC is a powerful and extensible incident response tool designed for forensic investigators, security analysts, and IT professionals. It automates the collection of artifacts from a wide range of Unix-like systems, including AIX, ESXi, FreeBSD, Linux, macOS, NetBSD, NetScaler, OpenBSD and Solaris.

> UAC v3.4.0 adds a sweeping set of forensic collectors for AI coding agents alongside new macOS persistence, Trash-directory, and AIX network-attribution artifacts, plus richer output from existing live_response process and network collectors.

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

01 **AI coding agent artifact collectors** NEW 95

UAC adds 18 new artifact definitions under `files/applications/ai_tools/` covering session data, configuration, and credentials for AI coding tools: `amp.yaml`, `claude_code.yaml` (session logs, config, credentials, pre-edit file history, tool results, auto-memory, plans, shell snapshots, hook scripts, IDE lock files), `claude_desktop.yaml` (transcripts, config, credentials, storage, skill/plugin definitions, app logs), `codebuff.yaml`, `codex.yaml` (OpenAI Codex CLI logs, config, auth, SQLite state/thread-history/log DBs with WAL/SHM sidecars, AGENTS.md, rules, shell snapshots, installation_id, excluding tmp/cache), `copilot.yaml` (OTEL usage logs, config, token store, session workspace metadata, plans/checkpoints, session store DB with WAL/SHM, VS Code Copilot Chat transcripts, agent-mode edit snapshots, extension session store), `cursor.yaml`, `droid.yaml`, `gemini.yaml` (chat logs, config, OAuth credentials, TOML commands/policies, GEMINI.md/memory, project root markers, excluding downloaded binaries/shadow git checkpoints/browser profile), `goose.yaml`, `hermes.yaml`, `kilo.yaml`, `kimi.yaml`, `kiro.yaml` (global config, MCP, agents, steering, prompts, skills, sessions, CLI/IDE data), `openclaw.yaml`, `opencode.yaml` (session data, config, credentials, SQLite WAL/SHM sidecars, logs, JSONC config, agent/command definitions, state directory, excluding node_modules/cloned repos/snapshots), `pi_agent.yaml`, and `qwen.yaml` (OAuth credentials). Most support linux and macos.

Collect forensic artifacts from all AI coding tools on a compromised developer workstation during an IR engagement.

```
$ ./uac -a ./artifacts/files/applications/ai_tools/* -p
ir_triage /tmp
```

— Names all 18 collector files with exact contents; runnable collection command given.

v3.4.0

02 **macOS PrivilegedHelperTools collector** NEW 65

Adds `files/system/macos_privilegedhelpertools.yaml` to collect macOS PrivilegedHelperTools, which may be used for persistence.

Collect macOS PrivilegedHelperTools to investigate potential persistence mechanisms on a macOS endpoint.

```
$ ./uac -a
./artifacts/files/system/macos_privilegedhelpertools.yaml /tmp
```

— Named file and purpose given, plus exact run command. v3.4.0

03 **Trash directory artifact collector** NEW 65

Adds `files/system/trash.yaml` to collect the entire Trash directory contents on freebsd, linux, macos, netbsd, and openbsd.

Collect Trash directory contents across all volumes to recover deleted evidence during a forensic investigation.

```
$ ./uac -a ./artifacts/files/system/trash.yaml /tmp
```

— Named file, platforms, and exact run command all given. v3.4.0

04 **AIX socket-to-process attribution via rmsock** NEW 65

Adds `live_response/network/rmsock.yaml` to identify process ownership for TCP network connections, associating PIDs with network activity on AIX systems where lsof is unavailable.

— Mechanism and platform limitation explained but no run example. v3.4.0

05 **Expanded live_response network and process command output**

IMPROVED 65

Extends `live_response/network/netstat.yaml` to include `netstat -Aan` on aix; extends `live_response/process/fstat.yaml` to include `fstat -n` on freebsd, netbsd, netscaler, and openbsd; and extends `live_response/process/ps.yaml` to include richer `ps -eo` output with `lstart`, `etime`, and `pcpu` / `pmem` columns across linux, macos, freebsd, netbsd, netscaler, openbsd, aix, and solaris.

— Exact commands and columns named but no usage example given. v3.4.0

THINNER COVERAGE BELOW

06 **Docker live_response collection on macOS** IMPROVED 35

Extends `live_response/containers/docker.yaml` artifact collection to macOS.

— Bare statement of platform extension, no further detail. v3.4.0

WAS THIS USEFUL? 👍 👎

◆ Malware Analysis

CAPEv2

Feedback ⓘ changes since 2026-08-23 CODE ↗

Malware Configuration And Payload Extraction

CAPEv2 improves Azure packet capture targeting for VMSS instances and refines Office/CAB file detection logic.

.
.

└──▷ TRY IT

Install the Azure sniffer dependencies using the new extras target instead of manually listing packages.

```
$ poetry install --extras azure
```

Run the CAPE installer with the built-in usage guide to see all available commands before choosing what to install.

```
$ bash installer/cape2.sh all 192.168.1.1 | tee cape2.sh.log
```

Targets specific Azure Virtual Machine Scale Set instances during packet capture by deriving instance ID from machine label, constructing a per-instance resource ID under `Microsoft.Compute/virtualMachineScaleSets/{vmss_name}/virtualMachines/{instance_id}`.

Excludes `MSI Installer` and `Microsoft Cabinet archive` file types from Office file detection via the new `MS_EXCLUDE` list in `lib/cuckoo/common/demux.py`, preventing CAB files from being misrouted to the Office password-protection branch.

Simplifies Azure dependency installation to `poetry install --extras azure` in `AzSniffer.py` error messaging.

Adds a structured usage() function to `installer/cape2.sh` documenting all installer commands including `Base`, `All`, `Sandbox`, `Dependencies`, `Systemd`, `Nginx`, `LetsEncrypt`, `Suricata`, `PostgreSQL`, `PostgreSQL_Utility`, `Yara`, and `Yara-x`.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

Security Onion

Feedback ⓘ 1 RELEASE · 2026-09-08 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 adds Logstash pipeline tuning controls in SOC, agentic memory with vector support for Agent Studio, and upgrades Elasticsearch to 9.4.5, alongside several Salt/state-management and installer reliability improvements.

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

01 **Logstash pipeline tuning in SOC** NEW 75

Adds tuning of multiple Logstash pipelines directly in SOC, including exposed `log.level` and `log.format` settings.

– Names exact config keys and location but no workflow detail 3.3.0-20260908

THINNER COVERAGE BELOW

02 **Grid-wide highstate push after soup upgrades** IMPROVED 50

Pushes a grid-wide highstate to remote nodes after a `soup` upgrade to ensure all nodes converge immediately.

– Names the `soup` command and explains the convergence mechanism 3.3.0-20260908

03 **Conflict detection for hand-placed files in Auto State Apply** IMPROVED 45

Detects hand-placed local/salt files during Auto State Apply to surface conflicts before they break state runs.

– Explains behaviour but no command or file path given 3.3.0-20260908

04 **Docker image reuse for airgap installs** IMPROVED 35

Allows airgap installs to reuse previously extracted Docker images, reducing re-extraction time.

– States benefit but no flag or command to invoke it 3.3.0-20260908

05 **Agentic memory with vector support in Agent Studio** NEW

30

Adds agentic memory capability with a vector extension for Agent Studio.

— Names the capability but not how it's used or configured 3.3.0-20260908

06 **Elasticsearch upgraded to 9.4.5** IMPROVED

30

Upgrades Elasticsearch to 9.4.5.

— Version bump only, no scope of changes given 3.3.0-20260908

07 **Log rotation for hypervisor logs** NEW

25

Adds log rotation for hypervisor logs.

— Bare description with no rotation policy or config details 3.3.0-20260908

WAS THIS USEFUL? 👍 👎

NETRESEC

Feedback ⓘ 1 RELEASE · 2026-09-08 BLOG ↗ RANK

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

> PolarProxy 2.0.2 adds SOCKS/Tor proxy chaining with a bypass mode for protocol-only conversion, granular idle and TLS-handshake timeout controls, environment-variable configuration for containerized deployments, and an SPDX SBOM, alongside a license keyfile flag, expanded PCAP-over-IP capture, and new build/packaging artifacts.

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

01 SOCKS/Tor proxy chaining and bypass mode NEW 88

PolarProxy can run as a local SOCKS and/or HTTP proxy that relays outgoing connections through an upstream proxy via `--connect socks4:HOST:PORT` or `--connect socks5:HOST:PORT` (or a plain `HOST` sinkhole), enabling use cases like decrypting your own HTTPS traffic before forwarding it through Tor with `--connect socks5:127.0.0.1:9050`. TLS is decrypted and re-encrypted by default unless `--bypass` is set, which uses PolarProxy purely as a protocol converter; HTTP proxy mode now decrypts and re-encrypts TLS traffic regardless of port.

Inspect your own HTTPS traffic before it enters the Tor network — decrypt TLS at PolarProxy and capture everything (including non-TLS) to a PCAP-over-IP stream for live analysis.

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

Inspect your own HTTPS traffic before it enters the Tor network, with full PCAP capture of all tunneled traffic including non-TLS flows.

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

Intercept and decrypt HTTPS traffic before forwarding it through Tor, with full PCAP capture of all tunneled traffic for offline analysis.

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

— Names flags and Tor address, gives runnable commands

PolarProxy 2.0.2 Released (2026-09-08)

02 **Environment-variable configuration and deployment packaging**

NEW

81

Supports uppercase `PP_` `-prefixed` environment variables as an alternative to all command-line arguments (e.g. `PP_SOCKS` mirrors `--socks`), suited for systemd, Docker, Podman, Kubernetes, and Helm deployments; `--helpenv` prints all supported variables. Ships a `docker-compose.yml` for musl builds or a systemd unit file installed via `install-polarproxy-service.sh` for non-musl Linux builds, both paired with a `polarproxy.env` configuration file.

Run PolarProxy in a container-friendly way using a `polarproxy.env` file instead of baking secrets and flags into the command line.

ini

```
# polarproxy.env
PP_SOCKS=1080
PP_PCAPOVERIP=57012
PP_IDLETIMEOUTCLIENT=120
PP_IDLETIMEOUTSERVER=120
```

Discover every environment variable PolarProxy supports before writing your deployment config.

```
$ PolarProxy --helpenv
```

Run PolarProxy in Docker with idle-timeout and SOCKS settings supplied via environment variables instead of command-line flags, keeping secrets out of process arguments.

ini

```
PP_SOCKS=1080
PP_CONNECT=socks5:127.0.0.1:9050
PP_IDLETIMEOUTCLIENT=120
PP_IDLETIMEOUTSERVER=120
PP_NONTLS=allow
```

Quickly audit which environment variables PolarProxy accepts before migrating from CLI flags to a container-friendly env-var config.

```
$ PolarProxy --helpenv
```

— Multiple named files/flags with config and CLI examples

PolarProxy 2.0.2 Released (2026-09-08)

03 **Idle and TLS handshake timeout flags** NEW 78

Adds `--idletimeoutclient <seconds>` and `--idletimeoutserver <seconds>` to close connections idle beyond a configurable period (no timeout by default) on the client and server sides, preventing zombie connections in long-running deployments. Adds `--tlstimeout <seconds>` (default 30 s) for a dedicated TLS-handshake deadline, complementing the existing `--timeout <seconds>` TCP-handshake flag.

Kill idle upstream connections after 120 s and enforce a 10 s TLS-handshake deadline to avoid zombie sessions accumulating in long-running proxy deployments.

```
$ PolarProxy --socks 1080 --tlstimeout 10 --idletimeoutserver
120 --idletimeoutclient 120
```

Drop zombie connections that have been idle to prevent resource exhaustion in long-running proxy deployments.

```
$ PolarProxy --socks 1080 --idletimeoutclient 120 --
idletimeoutserver 300
```

Kill stalled sessions automatically so long-running transparent proxy deployments do not accumulate zombie connections.

```
$ polarproxy --idletimeoutclient 60 --idletimeoutserver 120
```

— Three named flags with defaults and runnable examples

PolarProxy 2.0.2 Released (2026-09-08)

THINNER COVERAGE BELOW

04 **License key file loading via --keyfile** NEW 55

Adds `--keyfile <path>` flag to load a license key from a file rather than embedding it on the command line, enabling higher data/session limits.

Load a license key from disk to unlock higher session/data limits without embedding the key in a shell history or process list.

```
$ polarproxy --keyfile /etc/polarproxy/license.key
```

— Named flag with a runnable example command product docs

05 **Linux ARM build, release manifest, and container images** NEW

42

Adds a Linux ARM build alongside a release manifest with fixed version-specific download URLs and hashes for Linux builds, and publishes official container images at `ghcr.io/netresec/polarproxy` with deployment instructions at `https://github.com/Netresec/PolarProxy`.

– Names artifacts and URLs but no usage walkthrough `product docs`

06 **SPDX software bill of materials** NEW

38

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

– Names the file but no usage steps shown `PolarProxy 2.0.2 Released (2026-09-08)`

07 **Full-traffic PCAP-over-IP capture with --writeall** NEW

35

Adds `--writeall` flag to extend PCAP-over-IP output to include all proxied traffic, not just decrypted TLS.

– Named flag but no dedicated example or scope detail

`PolarProxy 2.0.2 Released (2026-09-08)`

08 **Debug output flag** NEW

26

Adds `--debug` flag to print debug output to STDERR, overriding `-v`.

– Bare flag description, no example given `product docs`

└──▷ ALSO FROM THESE RELEASES

Intercept and decrypt your own HTTPS traffic before it enters the Tor network — capture everything, including non-TLS flows, via PCAP-over-IP for live analysis.

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

WAS THIS USEFUL? 👍 👎

◆ Firewalls & Network Defense

Sophos Central Firewall

Feedback ⓘ 1 RELEASE · 2026-09-08

NOTES ↗ RANK

Sophos Central Firewall is a cloud-managed network security solution that provides centralized protection, threat prevention, and policy management across distributed firewalls.

> Sophos Central Firewall increased the maximum Central Firewall Reporting storage entitlement available to firewall models on term licences.

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

01 **Higher reporting storage entitlement for term-licence firewalls**

IMPROVED 30

The maximum Central Firewall Reporting storage entitlement for firewall models using term licences has been increased, allowing more reporting data to be retained before the storage limit is reached.

– States the change but no concrete new limit or numbers given.

2026.38Released on September 8, 2026

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

SpecterOps AzureHound

Feedback ⓘ 1 RELEASE · 2026-09-08

NOTES ↗ RANK

Azure Data Exporter for BloodHound

> AzureHound adds persistent, size-bounded log file collection with configurable rotation, compression, and pruning for long-running collection services.

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

01 **Log file rotation and retention flags** NEW 95

Adds `--log-file` to write logs to a file, with automatic rotation when the active log reaches `--log-max-size` MiB (default: 100 MiB); rotated logs are timestamped and stored beside the active log. Adds `--log-compress` to gzip-compress rotated archives (default: true), `--log-max-age` to prune archives older than a given number of days (default: 14; 0 disables age pruning), and `--log-max-backups` to cap the number of retained archives (default: 20; 0 disables count pruning).

Run a long-lived AzureHound collection service with bounded, compressed log rotation — keeping at most 30 archives no older than 7 days.

```
$ azurehound start --log-file /var/log/azurehound/azurehound.log
--log-max-size 50 --log-max-backups 30 --log-max-age 7 --log-
compress
```

— Names every flag with defaults and a runnable command v3.1.1

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

Chainguard

Feedback ⓘ 2 RELEASES · 2026-09-07 → 2026-09-09

CHANGELOG ↗ RANK

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

> Chainguard shipped Go 1.27 with runtime FIPS module selection, a Cloudsmith pull-through guide for Free and Production registries, a new free Catalog Starter plan, JFrog Catalog integration for Chainguard Libraries, and 39 additional container images.

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

01 Cloudsmith pull-through cache for Chainguard containers NEW

90

A new guide documents using Cloudsmith as a pull-through cache for Chainguard Free containers, by setting the upstream Proxy URL to `https://cgr.dev/chainguard` with Mode set to Cache and Proxy, and for Chainguard Production containers by setting Proxy URL to `https://cgr.dev/` and authenticating with a pull token generated via `chainctl auth configure-docker --pull-token`. A new `--ttl` flag on that command controls pull token lifetime (e.g. `--ttl=24h`; default 30 days), and Production images can then be pulled via `docker.cloudsmith.io/<cloudsmith-organization>/<cloudsmith-repository>/<chainguard-registry>/IMAGE`.

Generate a 7-day pull token for a Chainguard org registry to use as Cloudsmith upstream credentials.

```
$ chainctl auth configure-docker --pull-token --ttl=168h
```

Pull a Production container image from Chainguard through a Cloudsmith pull-through repository.

```
$ docker pull docker.cloudsmith.io/chainguard-example/chainguard-private/chainguard.edu/python:3.9-dev
```

— Exact config keys, flag and runnable pull command product docs

02 Chainguard Catalog Starter free plan and chainctl commands NEW

90

Introduces Chainguard Catalog Starter, a free standalone plan letting teams choose and pull up to five non-FIPS container images (including dependent Helm charts) without a paid subscription, pullable through third-party registries such as JFrog Artifactory and usable in CI/CD. New `chainctl starter init`, `chainctl starter request-access`, `chainctl starter add-images`, and `chainctl starter status` commands handle signup, joining an org, selecting images, and checking registry path, provisioning status, and quota usage; users are assigned the `limited_owner` role granting Console browsing, image pulling, and pull token creation.

Sign up for a new Catalog Starter account and select your free images entirely from the terminal.

```
$ chainctl starter init
```

Add specific images to your Catalog Starter plan after signup — for example, picking python and nginx as two of your five slots.

```
$ chainctl starter add-images python nginx
```

Check provisioning status and confirm all selected images are ready to pull before updating CI/CD pipelines.

```
$ chainctl starter status
```

— Names every CLI subcommand and role with runnable examples `product docs`

03 Go 1.27 across go, go-fips, go-openssl-fips images NEW

85

Adds Go 1.27 support to the `go` and `go-fips` container images, and introduces a new `go-openssl-fips` image that selects its FIPS-validated cryptographic module at deployment time rather than compile time — letting one artifact satisfy both the OpenSSL FIPS provider and Go Cryptographic Module requirements, with CNSA 2.0 readiness, without recompilation. Go 1.26 and earlier remain supported until end-of-life.

Build a single Go 1.27 binary that satisfies FedRAMP/CNSA 2.0 requirements — the validated FIPS module is chosen at deploy time, so one image runs across environments without recompilation.

```
$ FROM cgr.dev/chainguard/go-openssl-fips:latest AS build
RUN go build -o /app ./...

FROM cgr.dev/chainguard/go-openssl-fips:latest
COPY --from=build /app /app
ENTRYPOINT ["/app"]
```

— Names images, mechanism and a runnable Dockerfile Week of 2026-09-07

changelog-20260909-283b8cc5

THINNER COVERAGE BELOW

04 **JFrog Catalog integration for Chainguard Libraries** NEW

55

Chainguard-built packages are now recognized in JFrog Catalog, letting joint Chainguard and JFrog customers pull Chainguard Libraries through JFrog and use JFrog Zero-Touch Remediation to swap in patched Chainguard packages without developer workflow changes or major version upgrades. Java support ships at launch, with JavaScript and Python scheduled by end of September 2026.

— Explains benefit but gives no setup steps Week of 2026-09-07

changelog-20260909-283b8cc5

05 **39 new container images including Kubeflow Pipelines FIPS variants**

NEW

50

Adds 39 new container images this week, including 10 `kubeflow-pipelines-*-fips` images (`kubeflow-pipelines-api-server-fips` , `kubeflow-pipelines-cache-deployer-fips` , `kubeflow-pipelines-cache-server-fips` , `kubeflow-pipelines-driver-fips` , `kubeflow-pipelines-frontend-fips` , `kubeflow-pipelines-metadata-envoy-fips` , `kubeflow-pipelines-metadata-writer-fips` , `kubeflow-pipelines-persistenceagent-fips` , `kubeflow-pipelines-scheduledworkflow-fips` , `kubeflow-pipelines-viewer-crd-controller-fips`) plus `dbmate` , `hadolint` , `jruby` , `kserve-huggingfaceserver` , `gubernator` , `fortiotel` , `packer` , `security-profiles-operator` , `aws-lambda-dotnet` , `opentelemetry-go-instrumentation` , `prom-label-proxy` , `kserve-sklearnserver-fips` , `presidio-anonymizer` , and `redpanda-console-fips` , among others.

— Names images but no usage steps or mechanism Week of 2026-09-07

changelog-20260909-283b8cc5

WAS THIS USEFUL? 👍 👎

kubescape

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

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

> Kubescape v4.0.14 adds fleet-wide multi-cluster scanning with cross-cluster reporting, new control-listing filters, structured MCP error handling, and new/extended security detection rules.

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

01 Fleet-wide multi-cluster scanning and reporting IMPROVED

80

The `--kube-contexts` fleet mode in `kubescape scan` now supports framework, control, and workload scan targets across multiple clusters, not just full scans. Kubescape also adds cross-cluster control matrix and fleet report types to aggregate posture across a fleet of clusters.

Run a framework scan across multiple clusters simultaneously in fleet mode to get a cross-cluster posture view.

```
$ kubescape scan framework nsa --kube-contexts cluster-prod,cluster-staging,cluster-dev
```

— Names flag and new report types with example command v4.0.14

02 Framework and search filters for list controls NEW

70

`kubescape list controls` gains `--framework` and `--search` filters to narrow the control listing by framework or keyword.

Filter the control list to a specific framework to quickly find controls relevant to a compliance standard.

```
$ kubescape list controls --framework nsa
```

— Exact flags and runnable command given v4.0.14

THINNER COVERAGE BELOW

03 New and extended detection rules NEW

55

Adds the `host-users-root-workload-v1` rule to identify workloads running as host root users, and extends `provider-iam-assumption-v1` to detect Azure AKS Workload Identity.

— Names both rule IDs but no usage example v4.0.14

04 **Structured MCP server error responses** IMPROVED 40

The `kubescape mcpserver` MCP server now returns structured, machine-readable error responses.

— Names surface but no format detail or example v4.0.14

WAS THIS USEFUL? 👍 👎

Anchore

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

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

> Anchore introduced an Enterprise MCP server that gives AI agents native, structured access to vulnerability findings, policy results, and SBOM data.

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

01 **Anchore Enterprise MCP server for AI agents** NEW 50

The MCP server exposes curated MCP tools covering key API properties for specific security objectives such as triage, policy checks, and risk reporting, with a fallback to generic API invocation for broader coverage. It also handles large payload management, pagination, and consistent response handling automatically, letting agentic workflows query Anchore at scale without custom glue code.

— Describes mechanism and scope but names no concrete tool names, endpoints, or config.

Anchore + AI Just Got Easier: The Ancho…

WAS THIS USEFUL? 👍 👎

◆ CNAPP

Rapid7 InsightCloudSec

Feedback ⓘ 1 RELEASE · 2026-09-07

BLOG ↗ RANK

Rapid7 InsightCloudSec is a cloud security platform that provides visibility, compliance monitoring, and threat detection across multi-cloud environments.

> Rapid7 InsightCloudSec's 26.9.8 release focuses on Kubernetes visibility and detection tuning, updating the Kubernetes Scanner and adding new Insights and Query Filters alongside harvester performance work.

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

01 **New Kubernetes Scanner version** IMPROVED 20

InsightCloudSec 26.9.8 introduces a new Kubernetes Scanner version aimed at improved cluster resource coverage.

– No version number, mechanism, or scope of coverage given 2026-09-07-8323b07d

02 **New Insights for cloud security posture** NEW 20

Adds new Insights for cloud security posture assessment.

– No names of specific Insights or how many were added 2026-09-07-8323b07d

03 **Enhanced Query Filters** IMPROVED 20

Enhances existing Query Filters with additional filtering capabilities.

– No filter names or concrete capabilities listed 2026-09-07-8323b07d

04 **Harvester performance improvements** IMPROVED 20

Improves harvester performance and resource collection.

– No metrics or mechanism behind the performance gain 2026-09-07-8323b07d

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

World Monitor

Feedback ⓘ 1 RELEASE · 2026-09-08 NOTES ↗ RANK

Real-time global intelligence dashboard. AI-powered news aggregation, geopolitical monitoring, and infrastructure tracking in a unified situational awareness interface

> World Monitor's v2.10.0 release adds MCP agent endpoints for story corroboration and trade data, expands the Country Resilience Index with food, mineral and education data, and grows market panels, localization and company-monitoring capabilities.

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

01 **Country Resilience Index gains food, mineral and education data**

NEW 60

Ingests USDA food stocks data and exposes stocks-to-use ratios in the Country Resilience Index; adds mineral production and processing shares sourced from USGS MCS and BGS; and activates the education dimension, including a flag-dark education dimension.

— Names data sources and metrics but no UI location. v2.10.0

THINNER COVERAGE BELOW

02 **MCP agent endpoints for story corroboration and dashboard control**

NEW 55

Exposes story corroboration to agents via MCP (`feat(mcp): expose story corroboration to agents`) and exposes WTO trade flows to agents via MCP, naming coverage-collapse causes. Also adds safe live dashboard controls for agents via `webmcp` .

— Names MCP surfaces but gives no endpoint schema or usage. v2.10.0

03 **Market panel expansion: RUB FX tab, provider chain, correlation, watchlists**

IMPROVED 55

Adds the RUB quote table as a third FX panel tab; authorizes Finnhub and AV as a quote provider chain for markets; correlates news volume with market returns in market panels; and adds visual stock and market watchlist customization.

— Named providers and tab but no config or command shown. v2.10.0

04 **Company monitoring pipeline: discovery, onboarding, scoring and evidence**

NEW

50

Adds bounded Exa cohort discovery and bounded portfolio onboarding for company monitoring, durable scan orchestration, classification and admission of material impacts, normalization of scoped evidence candidates, sealed offline prediction custody, and ingestion of verified X posts.

— Lists many sub-capabilities without mechanism or interface names. v2.10.0

05 **UI font scaling and new locale support** NEW

45

Adds global and per-panel font scaling to the UI, plus new locale support for Traditional Chinese (`zh-TW`) and Swahili.

— Names locales but no settings path or toggle given. v2.10.0

06 **Preflight system dependency checking** IMPROVED

35

Adds preflight system dependency checking instead of failing mid-build.

— Explains behavior change but no command or check list. v2.10.0

07 **Defense industrial intelligence in military monitoring** NEW

25

Adds defense industrial intelligence to the military monitoring surface.

— Bare feature name with no mechanism or scope. v2.10.0

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Elastic Detection Rules

Feedback ⓘ 1 RELEASE · 2026-09-08

NOTES ↗ RANK

Detection Rules is Elastic's framework for creating and managing security detection logic to identify threats and anomalies in monitored systems.

> This release added over 30 new detection rules spanning AWS, GCP, identity, network, and endpoint threats across Linux, macOS, Windows and Kubernetes, alongside free text search support in KQL for building detection queries.

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

01 **New AWS and GCP cloud detection rules** NEW 55

Adds new detection rules: AWS Root Console Login Password Spraying, AWS S3 Bucket MFA Delete Disabled, AWS Organizations Delegated Administrator Registered, AWS Service Quota Increase Requested by Rare Identity, AWS Backup Resource Enumeration via Long-Term Access Key, AWS SES Enumeration via Long-Term Access Key, AWS SES Identity Verified Then Deleted, AWS SES Full Access Policy Attached to IAM Entity by Unusual User, AWS Bedrock AgentCore Resource Created with IAM Execution Role, AWS GetFederationToken Followed by Console Login via Federation Exchange, AWS GuardDuty Threat Intelligence Set Deleted, AWS GuardDuty Publishing Destination Deleted, AWS EKS Access Entry Created Then Deleted by Same Identity, AWS Detective Graph Deleted, and GCP IAM Service Account Impersonation Role Granted.

– Rule names given but no query logic or triggering conditions dev-v2.2.0

02 **Endpoint detection rules for Linux, macOS and Windows** NEW 50

Adds new detection rules: Suspicious Process Execution by Zoom on macOS or Linux, File Downloaded by Curl/Wget and Piped to Interpreter, Process Execution Followed by Self-Deletion, Kernel Module Loaded with Tainting Flags, Procfs Syscall Read and binfmt Configuration File Creation, Claude Cowork VM Boot Image Tamper, and Potential Evasion via Boot Time Removal Tool.

– Rule names given but no detection logic detailed dev-v2.2.0

03 **Identity and Active Directory detection rules** NEW 45

Adds new detection rules: Potential Entra ID PRT Extraction via BrowserCore, PKINIT Followed by Same-Principal U2U Service Ticket, and Potential CertiGhost AD CS Machine Identity Mismatch.

– Rule names given but no detection logic detailed dev-v2.2.0

04 **Network and TLS detection rules** NEW 45

Adds new detection rules: `Potential DNS Tunneling via Long and Unique Subdomains`, `Potential DNS Rebinding from Public to Private Address`, `Self-Signed TLS Certificate Recently Issued on External Connection`, and `First Seen SonicWall Remote Access Login by User and Source`.

— Rule names given but no detection logic detailed dev-v2.2.0

05 **Free text search support in KQL** NEW 40

Detection rule queries can now use free text support in KQL, adding a new query capability for building detection logic.

— No syntax example or affected fields given dev-v2.2.0

06 **New Kubernetes hunting query for AKS** NEW 30

Adds a new hunting query, `AKS Kubelet nodes/proxy Command Execution from an External Source IP`.

— Single named query with no detection logic detailed dev-v2.2.0

WAS THIS USEFUL? 👍 👎

Tenzir

Feedback ⓘ 1 RELEASE · 2026-09-08 BLOG ↗ RANK

Tenzir is a data pipeline engine for security teams that collects, transforms, enriches, and routes telemetry.

> Tenzir's v6.16.0 window centers on automatic Sigma-to-OCSF rule matching, alongside new Microsoft 365 and Kafka Avro ingestion, expanded Entra workload identity federation for Azure Blob Storage, ClickHouse query pushdown, a new blob conversion function, and smaller diagnostics/performance fixes.

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

01 Automatic Sigma-to-OCSF rule matching NEW

98

Adds automatic OCSF matching for the `sigma` operator: OCSF-shaped table schemas (identified by `metadata.version` string and `class_uid` int64/uint64) are matched structurally using a built-in mapping catalog covering Sysmon-backed Windows categories, Linux/macOS process creation, Windows Security/System/PowerShell/Defender channels, Okta, Entra ID, Azure activity logs, AWS CloudTrail, GCP Cloud Audit Logs, and Zeek DNS/HTTP/SMB; use `mapping="direct"` to opt out of structural matching for literal field matching. Sigma rule diagnostics also now point directly at the offending rule.

Run Sigma rules against an OCSF event stream automatically; opt out of structural OCSF mapping when you need literal field matching instead.

```
$ subscribe "ocsf"
| sigma path = "sigma/rules" mapping="direct"
```

— Names schema fields, mapping catalog scope, and opt-out flag with example

Tenzir Node v6.16.0: Automatic Sigma Ma…

02 Entra workload identity federation for Azure Blob Storage NEW

95

Adds an `azure_auth` record with a `web_identity` field to `from_azure_blob_storage` and `to_azure_blob_storage`, supporting Entra workload identity federation via `token_endpoint`, `token_file`, or inline `token` — covering GitHub Actions, GCP metadata server, and Kubernetes projected service account tokens — so a single node can operate across multiple Entra tenants simultaneously. A new `query_params` record on `web_identity.token_endpoint` lets OIDC audience parameters (e.g. `'audience': 'api://AzureADTokenExchange'` for GitHub Actions or `'sts.amazonaws.com'` for AWS) be passed without manual URL concatenation, accepting both `string` and `secret` values.

Read from an Azure Blob Storage path using Entra workload identity federation from a GitHub Actions runner, scoped to a specific customer tenant.

```
$ from_azure_blob_storage
"abfss://logs@customer1.dfs.core.windows.net/**.json.gz"
  azure_auth = {
    tenant_id: secret("customer1-entra-tenant")
    client_id: secret("customer1-entra-client")
    web_identity: {
      token_endpoint: {
        url: env("ACTIONS_ID_TOKEN_REQUEST_URL")
        query_params: { "audience": "api://AzureADTokenExchange"
}
        headers: { "Authorization": "Bearer " +
env("ACTIONS_ID_TOKEN_REQUEST_TOKEN") }
        path: ".value"
      }
    }
  }
| read_json
```

— Names config fields, token sources, and includes runnable example

Tenzir Node v6.16.0: Automatic Sigma Ma…

03 **Microsoft 365 audit activity collector** NEW 93

Adds `from_microsoft_365_activity` operator to collect unified audit records from Microsoft 365, handling Activity API subscriptions, backfills, continuous polling, pagination, retries, and snapshot-backed blob checkpoints; configured with `auth` (`tenant_id` , `client_id` , `client_secret`) and `content_types` (e.g. `['Audit.General']`).

Continuously collect Microsoft 365 general audit events into the pipeline as they arrive, using secret-backed credentials.

```
$ from_microsoft_365_activity
  auth = {
    tenant_id: secret("m365-tenant-id")
    client_id: secret("m365-client-id")
    client_secret: secret("m365-client-secret")
  }
  content_types = ["Audit.General"]
```

— Names operator, config fields, and shows a runnable pipeline example

Tenzir Node v6.16.0: Automatic Sigma Ma…

04 **ClickHouse filter, limit and field pushdown** IMPROVED

83

Adds filter, limit (`head`), and field selection (`select`) pushdown from `from_clickhouse` into ClickHouse SQL queries, translating predicates to `WHERE` , column lists to selected columns, and row limits to `LIMIT` ; falls back to local evaluation for unsupported expressions (function calls, `time` / `ip` comparisons, `Enum` / `Decimal` types), reducing data transferred from upstream.

— Names operator and exact SQL translation mechanics, no runnable example

Tenzir Node v6.16.0: Automatic Sigma Ma…

05 **Kafka Avro decoding via Schema Registry** NEW

83

Adds a `schema_registry` parameter to `from_kafka` for direct Avro decoding, supporting Confluent schema IDs in payload prefixes and schema GUIDs in Kafka headers, with independent registry authentication and TLS settings.

— Names the config parameter and encoding details, lacks a worked example

Tenzir Node v6.16.0: Automatic Sigma Ma…

THINNER COVERAGE BELOW

06 **blob conversion function** NEW

45

Adds a `blob` function that converts UTF-8 strings to blobs without encoding the payload.

— Names the function but gives no usage example or scope

Tenzir Node v6.16.0: Automatic Sigma Ma…

07 **Source locations in startup diagnostics** IMPROVED

23

Node startup diagnostics now include source locations, easing troubleshooting of startup errors.

— Bare mention, no mechanism or location detail given

Tenzir Node v6.16.0: Automatic Sigma Ma…

08 **Faster catalog match-all lookups** IMPROVED

21

Improves catalog lookups with a faster match-all path.

— One-line perf note with no numbers or mechanism

Tenzir Node v6.16.0: Automatic Sigma Ma…

WAS THIS USEFUL? 👍 👎

◆ SIEM

Databricks

Feedback ⓘ 5 RELEASES · 2026-09-07 → 2026-09-08 BLOG ↗

RANK

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

> Databricks shipped Unity Catalog ABAC DENY policies in Beta, upcoming behavior changes to Salesforce ingestion in Lakeflow Connect, expanded Lakebase compliance coverage, a new time_bucket SQL function, and Public Preview support for Zerobus Ingest into default storage.

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

01 **time_bucket SQL function** NEW 78

Adds the `time_bucket` SQL function, which returns the start of a fixed-width interval (e.g. 15-minute or 3-month buckets) aligned to a caller-specified origin, for cases where `date_trunc` calendar units are too coarse or misaligned.

— Names function, example intervals, and comparison to date_trunc

time_bucket SQL function aligns timesta…

02 **Lakebase PCI-DSS and HITRUST in all AWS regions** IMPROVED 65

Lakebase now extends PCI-DSS and HITRUST compliance to all AWS regions where Lakebase is available, for workspaces with the compliance security profile enabled — previously this was limited to `us-east-1`.

— Names prior region limit and required workspace profile setting

Lakebase now supports PCI-DSS and HITRU…

03 **ABAC DENY policies in Unity Catalog** NEW 62

Unity Catalog adds ABAC DENY policies (Beta) that can explicitly deny the `MANAGE ACCESS CONTROL` privilege to specified principals, including object owners, and these deny policies always take precedence over any grant.

— Names the privilege and precedence behavior but no config steps

ABAC DENY policies are in Beta (2026-09…

THINNER COVERAGE BELOW

04 **Incremental ingestion default for Salesforce formula fields** 50

BREAKING

Lakeflow Connect will soon default to incremental ingestion for Salesforce formula fields instead of taking a full snapshot on every pipeline run, improving performance and reducing cost. This is a breaking change on GA: existing pipelines relying on the full-snapshot default will change behavior on upgrade.

.
.
.

— Describes upcoming behavior change but no migration steps given

Incremental ingestion for Salesforce fo…

05 **Zerobus Ingest into default storage** NEW 40

Lakeflow Connect's Zerobus Ingest now supports ingesting into tables backed by default storage, now in Public Preview.

— Names the feature and preview status but no usage detail

Zerobus Ingest into default storage is …

└──▷ **BREAKING ON UPGRADE**

! When incremental Salesforce formula field ingestion reaches GA, full snapshots will no longer be the default for Lakeflow Connect pipeline runs — existing pipelines that relied on the full-snapshot default will change behavior on upgrade.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Trend Vision One

Feedback ⓘ 4 RELEASES · 2026-08-24 → 2026-09-08

BLOG ↗ RANK

Trend Vision One is Trend Micro's cloud-based XDR platform providing unified security visibility and threat detection across endpoints, networks, and cloud environments.

> Trend Vision One added AI-powered filter recommendations to Intrusion Prevention Configuration, significantly expanded asset- and workload-based vulnerability filtering and owner notifications in Security Playbooks, and enabled custom resource tagging for OCI in Cloud Accounts.

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

01 Asset-based vulnerability filtering and notifications in Security Playbooks

NEW 85

Security Playbooks gain asset attribute conditions for filtering vulnerabilities — asset group, custom tags, criticality, device service, operating system, application, and CVSS score — plus container-specific conditions (cluster name, namespace, group, custom tags) and cloud workload vulnerability conditions covering CVSS score ranges, global exploit potential, exploit detection status, and prevention rule coverage. Automated notification routing to asset owners can now trigger directly from playbook workflows based on asset ownership models and custom tags, and playbooks for CVEs with global exploit potential now extend this filtering to containers and cloud VMs for more precise stakeholder notifications and faster remediation.

Build a playbook that fires when a critical cloud workload vulnerability with active exploit detection is discovered, then automatically notifies the asset owner — reachable via Workflow and Automation → Security Playbooks.

📍 In Trend Vision One, go to Workflow and Automation → Security Playbooks → New Playbook. Add a trigger condition: set Exploit Detection Status = detected, CVSS Score >= 9.0, and Criticality = critical. Add an action step: Notify Asset Owner using the asset's ownership metadata. Save and activate the playbook.

Navigate to the security playbooks area to configure or review CVE playbooks that now apply to containers and cloud VMs.

📍 In the console, go to Workflow and Automation → Security Playbooks, locate a CVEs with global exploit potential playbook, and update the asset scope to include containers and cloud virtual machines (VMs).

— Names every playbook condition added; only UI steps shown, no API

Asset-based vulnerability filtering and… | Expand CVEs with global exploit activit…

02 Custom resource tagging for OCI in Cloud Accounts NEW

65

Cloud Accounts now supports custom key-value resource tagging for Oracle Cloud Infrastructure (OCI) deployments, configurable as Terraform variables or through the Trend Vision One console under Cloud Security → Cloud Accounts.

Apply org-required cost-attribution tags to all OCI resources at deployment time so you meet tagging policy without post-deploy manual edits.

> 📍 In the console, go to Cloud Security › Cloud Accounts, select your OCI account, and supply the required key-value tag pairs (for example, `CostCenter=infosec`, `Environment=prod`) in the custom resource tagging section before deploying.

— Names Terraform variable option and exact console path

Cloud Accounts now supports custom reso…

THINNER COVERAGE BELOW

03 AI-recommended actions in Intrusion Prevention Configuration

NEW

55

Intrusion Prevention Configuration now surfaces AI-powered security action recommendations that analyze threat landscape, network behavior, and current filter deployments to suggest optimal protection strategies and prioritize recommended action filters. Accessible via Network Security > Intrusion Prevention Configuration.

Review AI-generated filter prioritization recommendations to accelerate enabling inline intrusion prevention without manually auditing every filter.

> 📍 In the console, go to Network Security › Intrusion Prevention Configuration and review the AI-recommended security actions panel to identify which recommended action filters to enable based on your detected risks and network context.

— UI path given but no config key or API detail | Intrusion Prevention Configuration now …

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines

Feedback ⓘ 1 RELEASE · 2026-09-09 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 43.2.0 adds programmatic case management via the API, exposes case operations to its MCP surface, and extends formula support to AI provider URLs and case fields, alongside a round of storyboard, dashboard and change-control workflow improvements.

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

01 **Case creation and management in storyboard** NEW 57

The storyboard now supports visual case creation directly within it, formula support for case details fields, case notifications when comments on a case are updated, and priority labels in the cases list view.

– Names four distinct storyboard case additions but no deeper mechanism.

changelog-20260909-1fd54070

02 **Change control workflow enhancements** IMPROVED 47

Change control now supports adding comments to the change control workflow, and new stories can be renamed under change control without requiring approval.

– Two concrete workflow changes named, but no config detail. changelog-20260909-1fd54070

03 **Dashboard draft and edit mode** NEW 45

Dashboards gain a draft and edit mode, letting users stage dashboard changes before publishing them.

– Clear UI behaviour described but no navigation path given. changelog-20260909-1fd54070

04 **Cases tools in Tines MCP** NEW 43

Tines MCP now includes Cases tools, exposing case management operations to the Model Context Protocol surface.

– Names the MCP surface but not which specific tools/operations.

changelog-20260909-1fd54070

05 **Formula support for AI provider URLs** NEW 42

AI provider URLs now support formulas, enabling dynamic construction of provider endpoints at runtime.

– Explains the mechanism but gives no example or usage path. changelog-20260909-1fd54070

06 **Case fields updatable via the API** NEW 39

Case fields can now be modified programmatically through the Tines API (Update case fields via the API).

— Names the API surface but no endpoint or method given. changelog-20260909-1fd54070

07 **Audit log retention period configuration** NEW 35

Operators can now configure how long audit logs are retained, via a new audit log retention period setting.

— Describes the capability but not the config surface used to set it.

changelog-20260909-1fd54070

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

defectdojo

Feedback ⓘ 1 RELEASE · 2026-09-08 NOTES ↗ RANK

Open-Source Unified Vulnerability Management, DevSecOps & ASPM

> DefectDojo 3.3.0 significantly expands Rules Engine 2.0 and the Sensei AI assistant, adds a typed Custom Fields feature with a new API endpoint, broadens asset management and connector coverage (GHAS, OpenVAS/Greenbone, Wiz, Qualys, Smart Upload), and retires the classic sidebar in favor of the new navigation.

└──▷ **WHAT SHIPPED · 19 FEATURES** most completely described first ? what's the number?

01 **Typed Custom Fields with API endpoint** NEW 78

Adds a typed Custom Fields feature with support on create and edit forms, plus a new `GET /api/v2/` Custom Fields API endpoint for retrieving field definitions.

Query the new Custom Fields API to retrieve all custom field definitions for your instance.

```
$ curl -s -H 'Authorization: Token <your_api_token>'
https://<defectdojo_host>/api/v2/custom_fields/
```

— Endpoint and example command given, ready to use. 3.3.0

02 **Rules Engine 2.0 condition, trigger and action expansion** NEW 71

Rules Engine 2.0 gains new condition fields for KEV status and `exploit-evidence`, plus `reachability` and `asset-exposure` conditions; a `missing-scan` trigger; SLA configuration and Risk Priority asset actions; support for custom fields; and general asset support.

— Names many condition fields but no exact UI steps. 3.3.0

03 **Sensei AI assistant feature buildout** NEW 65

The Sensei AI feature adds AI Model Settings with LLM provider configuration, a Claude Code plugin page (with a corrected MCP tool count), a CSPM cloud-posture page with hub views and fix-quota states, inline repo association with a locate-the-file fix flow, and AI agent skill scanning.

— Lists Sensei sub-features without exact config or commands. 3.3.0

04 **Connector coverage across GHAS, OpenVAS, Wiz, Qualys, Smart Upload**

NEW

63

Connector coverage expands across several integrations: GitHub issue import support in the GHAS connector, GMP over SSH support in the OpenVAS/Greenbone connector, Wiz imports without Projects via a tenant-level Record, a Qualys Host Tags filter in the Qualys connector, and multi-Asset finding fan-out in Smart Upload.

— Names five connectors and their specific additions. 3.3.0

THINNER COVERAGE BELOW

05 **Asset management: bulk edit, exports, versions, hierarchy** NEW

59

Asset management gains a Bulk Edit action on the All Assets list, SBOM export and inventory export from the Asset page, Asset Versions with per-version claims in the UI, asset-hierarchy relationship types with direct vs indirect vulnerability views, and location inventory tracking sourced from asset connectors.

— Names asset UI features but no config/API given. 3.3.0

06 **API request body validation hardening** IMPROVED

50

Adds request-body validation on the finding metadata `PUT` endpoint, and validates the Jira epic action body while rejecting reserved dispatch kwargs.

— Names endpoint and action body but no scope detail. 3.3.0

07 **Reporting: chart blocks and quick export** NEW

46

Reporting gains Chart blocks (previously marked coming soon) and a Quick Export dialog that produces a named report directly from the findings view.

— Names UI dialog and chart blocks, no API detail. 3.3.0

08 **PAIN-keyed FedRAMP VDR remediation deadlines** NEW

41

Adds PAIN-keyed FedRAMP VDR remediation deadlines to the federal feature.

— Names federal feature and PAIN keying, no workflow detail. 3.3.0

09 **Downstream API v3 assets router write schemas** NEW

40

Lets a downstream distribution supply the assets router's write schemas via API v3.

— Names API v3 assets router but no schema detail. 3.3.0

10 **PSIRT feed rules and advisory workflow** NEW

38

PSIRT gains Feed Rules, a no-SBOM matching path, and an advisory-to-case workflow.

— Named PSIRT additions but no mechanism detail. 3.3.0

11 **Automatic mitigation from Dependency Track** IMPROVED

38

Finding mitigation is now set automatically from Dependency Track affected version ranges.

– Names source tool but no matching logic detail. 3.3.0

12 **Classic sidebar retired** BREAKING 35

The classic sidebar navigation is retired in 3.3.0; installations relying on it must migrate to the new sidebar.

– States retirement but no migration steps given. 3.3.0

13 **Organization type-scoped roles and grants** NEW 34

Adds a type-scoped grants UI for organizations and roles scoped to an organization type.

– Bare mention of grants/roles UI, no mechanism. 3.3.0

14 **Documentation surfaces and localized guides** NEW 33

Adds documentation surfaces for asset exposure and deployment context and for Form Configuration navigation, an RFC 9116 `security.txt` on `docs.defectdojo.com`, and Brazilian Portuguese, Simplified Chinese, Italian, and German translations of the core guides.

– Lists doc/translation additions, no operational surface. 3.3.0

15 **Connector health and membership notifications** NEW 28

Adds a Connector Health Warning notification type and notifications sent following every organization membership change.

– Named notification types only, no config detail. 3.3.0

16 **MFA disabling requires verification code** IMPROVED 26

Disabling MFA now requires a verification code rather than being immediate.

– States the change but no rollout or scope detail. 3.3.0

17 **Locations backfill cancel hook** IMPROVED 25

Adds a cancel hook to the endpoints-to-locations backfill (feat(locations)).

– Named backfill hook but no usage detail. 3.3.0

18 **Customizable page layouts on view pages** NEW 22

Adds customizable page layouts on view pages.

– Bare mention of layout customization, no options given. 3.3.0

19 **Changelog RSS feed** NEW 15

Adds an RSS feed to the changelog.

— Bare one-line addition with no further detail. 3.3.0

└──▷ BREAKING ON UPGRADE

! The classic sidebar is retired in 3.3.0 — installations relying on the classic sidebar navigation will need to migrate to the new sidebar.

WAS THIS USEFUL? 👍 👎

◆ Attack Surface & Exposure Management

Censys

Feedback ⓘ 1 RELEASE · 2026-09-08 BLOG ↗ RANK

Censys is a search engine for internet-connected devices and certificates that helps security researchers discover and analyze exposed infrastructure.

> Censys shipped an AI asset label for exposed AI tooling, a SentinelOne integration for enrichment and pivoting, an interactive host distribution map, and 14 new fingerprints and ASM risk detections.

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

01 New fingerprints and ASM risk detections NEW 80

Nine new fingerprints were added to the Platform: IServ, Liquidsoap, SonicWall Analytics, SonicWall Analyzer, SonicWall Global Management System, Zbtlink MQWrt Router, Dinky, RabbitMQ Management, and Zimbra Collaboration. Five new ASM risk fingerprints were also added: End-of-Life SonicWall Global Management System, End-of-Life SonicWall Analyzer, End-of-Life SonicWall Analytics, Vulnerable Cacti Server [CVE-2026-40079], and Vulnerable Zimbra Collaboration Server [CVE-2026-73570]. New risk types may be disabled by default and can be enabled via ASM Settings > Risk Type Configuration.

Identify hosts in your ASM workspace running end-of-life SonicWall management infrastructure before the September 2026 support deadline passes.

```
$ risks.name:`End-of-Life SonicWall Global Management System`
```

Review all newly added ASM risk types — including the five new fingerprints — before they appear in your risk dashboard, since new risk fingerprints may be disabled by default.

> 📍 In the ASM web console, go to Settings › Risk Type Configuration and review any risk types marked as disabled to enable the new End-of-Life SonicWall and Vulnerable Cacti/Zimbra risks for your workspace.

— Enumerates every fingerprint and risk with CVEs and enable steps

September 8, 2026 (2026-09-08)

THINNER COVERAGE BELOW

02 AI asset label in ASM NEW 55

A new `ai` label for host services and web entities in ASM surfaces exposed AI-related assets, covering tools including Ollama, Flowise, Langflow, LibreChat, ComfyUI, ChromaDB Admin, BentoML, Dify, FastGPT, LiteLLM, and MLflow.

— Names the label and covered tools but no query syntax shown

September 8, 2026 (2026-09-08)

03 SentinelOne integration for enrichment and pivoting NEW

55

A new SentinelOne integration automatically or manually enriches IPs, web properties, and certificates in SentinelOne with Censys Platform data, can initiate rescans, retrieve scan history for an IP, and launch CensEye automated pivoting jobs.

— Describes mechanism and capabilities but no setup steps given

September 8, 2026 (2026-09-08)

04 Interactive host distribution map in Platform search NEW

50

Platform search results now include an interactive Host Distribution world map visualization, with a Select Area filter to spatially narrow host query results.

— Names the UI filter but no exact navigation path given September 8, 2026 (2026-09-08)

WAS THIS USEFUL? 👍 👎

runZero

Feedback ⓘ 1 RELEASE · 2026-09-08 BLOG ↗ RANK

runZero is a cloud-based asset discovery and inventory platform that identifies and maps all connected devices across networks continuously.

> runZero's window centers on a new custom-roles and account-bound API client system spanning users, groups, SSO, and MCP connections, alongside UI-driven task reprocessing, SAML certificate expiry alerts, several asset-discovery and fingerprinting refinements, and a breaking change to NetBIOS-based hostname resolution.

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

01 Custom roles for users, groups, and API clients NEW

75

Custom roles are now definable on the Roles page, granting exact permissions that can be assigned as a user's default role, a per-organization role, a group role, the SSO enrollment default, locked to an API client, or applied to MCP connections.

— Names the Roles page and every assignment scope, no API detail

runZero 5.1.260908.0 (2026-09-08)

02 Account-bound API clients with granular permissions NEW

75

New account-bound API clients are managed on the API clients page as credentials with an explicit set of permissions and organizations that are not tied to any user account. Users can create API clients with custom permissions capped by their own access rights, and account-level API clients can use granular authentication scopes in addition to roles.

— Names the API clients page and permission-capping mechanism

runZero 5.1.260908.0 (2026-09-08)

03 Reprocess tasks directly from the UI NEW

75

Completed tasks can now be reprocessed directly from the runZero console to re-evaluate asset data without re-running the scan, useful after updating fingerprints or import configurations. In the console, open the task inspection card for a completed task and click Reprocess to trigger it.

Reprocess a completed task to re-evaluate asset data without re-running the scan — useful after updating fingerprints or import configurations.

> 📍 In the runZero console, open the task inspection card for a completed task, then click Reprocess to trigger reprocessing directly from the UI.

– Exact UI navigation steps provided in usage example runZero 5.1.260908.0 (2026-09-08)

04 **Asset discovery, hostname, and fingerprinting improvements**

IMPROVED 70

Recent assets now include sub-assets identified through protocol gateways; task summaries clearly indicate when a task involved more than 1,000 asset changes; WS-Discovery XAddr endpoints now contribute to asset hostnames; MAC vendor information is now populated for legacy MAC prefixes; AWS, Azure, and GCP imports include additional asset types; and Dragos and Wiz imports now apply more complete fingerprinting and OS CPE matching when available.

– Names six concrete improvements but no config keys runZero 5.1.260908.0 (2026-09-08)

THINNER COVERAGE BELOW

05 **MCP connections improved for Claude Desktop and API usage**

IMPROVED 50

MCP connections now work smoothly with Claude Desktop and similar tools, and background MCP connections no longer count against API usage.

– Names integration partner but no config surface given runZero 5.1.260908.0 (2026-09-08)

06 **NetBIOS hostname fallback removed** BREAKING 50

Hostname discovery no longer falls back to NetBIOS domains — assets whose hostnames were previously derived from NetBIOS domains will have those hostnames removed or changed.

– States before/after impact but no migration guidance runZero 5.1.260908.0 (2026-09-08)

07 **Email warnings before SAML certificate expiry** NEW 35

Account administrators now receive email warnings before SAML certificates expire.

– Thin description with no lead time or threshold runZero 5.1.260908.0 (2026-09-08)

└──▷ BREAKING ON UPGRADE

! Hostname discovery no longer falls back to NetBIOS domains, which may change hostnames for assets previously resolved via NetBIOS.

! Hostname discovery no longer falls back to NetBIOS domains — assets whose hostnames were previously derived from NetBIOS domains will have those hostnames removed.

WAS THIS USEFUL? 👍 👎

Intruder

Feedback ⓘ changelog · Sep 9, 2026 CHANGELOG ↗

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

Intruder adds Additional Domains configuration for authenticated web app scans, enabling subdomain and cross-domain coverage.

└──▷ HOW TO FIND IT

Ensure an authenticated scan of `app.example.com` also crawls and tests `api.example.com` and an external identity provider, so API backends and auth flows aren't skipped.

> 📍 In the Intruder console, open your web app target › Authentication settings › locate the Additional domains field › add `api.example.com` and your identity provider URL › save and re-run the scan.

Adds an Additional domains field when setting up or editing authentication for a web app target, allowing subdomains (e.g. `api.example.com`, `auth.example.com`) and external service URLs to be included in authenticated scan scope.

Supports cross-domain scan coverage for external services an application depends on, such as identity providers, CDNs, or third-party APIs, preventing blocked requests from causing missed vulnerabilities.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Didit

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

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

> Didit's biggest addition this window is a non-document ID Verification method — verifying users via national ID number and personal details instead of a photo — along with the per-country controls, fallback rules, retry limits, and automatic biometric checks needed to run it, plus a fix for embedded SDK sizing.

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

01 Configurable fallback behavior for lookup failures NEW

75

Adds configurable fallback behavior for each non-document method failure mode — partial match, no match, no source response, and cancelled/timed-out wallet sign-in — with each independently set to either send the user to document capture or decline the session.

Enable non-document lookup for a specific country so users can verify with just their national ID number and personal details — no document photograph required.

> 📍 In the console, open your workflow, select the ID Verification step, go to the Countries tab, choose the target country, and toggle Non-document lookup on. Set the fallback for each failure mode (partial match, no match, no source response) to either Document capture or Decline session, then save.

— All four failure modes and both outcomes named with console steps

changelog-20260909-fa2957ab

02 Per-country method controls for ID Verification NEW

70

Adds per-country method controls on the Countries tab of the ID Verification step, letting admins toggle document capture, non-document lookup, and (future) digital ID wallets on or off per country; the same settings are also available through the API.

Enable non-document lookup for a specific country so users can verify with just their national ID number and personal details — no document photograph required.

> 📍 In the console, open your workflow, select the ID Verification step, go to the Countries tab, choose the target country, and toggle Non-document lookup on.

> Set the fallback for each failure mode (partial match, no match, no source response) to either `Document capture` or `Decline session`, then save.

— Exact UI location and API parity named `changelog-20260909-fa2957ab`

---

03 **Embedded SDK sizing fix** IMPROVED 70

Embedded SDK mode now fills the host element's content box instead of inheriting the modal's height cap, fixing clipping on short or landscape viewports; update via `npm install @didit-protocol/sdk-web@latest`.

Upgrade the Web SDK so the modal no longer clips on short or landscape viewports and embedded mode fills your container correctly.

```
$ npm install @didit-protocol/sdk-web@latest
```

— Runnable install command and clear before/after behavior `changelog-20260909-fa2957ab`

---

04 **Retry configuration for non-document lookups** NEW 65

Adds retry configuration for non-document lookups: one to five attempts allowed (default two), counting only attempts the source actually answered; format-check failures never reach the source and are not billed.

— Exact retry range and billing rule given, no config step shown

`changelog-20260909-fa2957ab`

---

05 **Automatic biometric checks on non-document lookups** NEW 60

Adds automatic selfie capture, passive liveness detection, and portrait matching to non-document lookups for countries whose government register returns a photograph (South Africa, Nigeria, Argentina, Panama), included in the lookup price at no extra cost.

— Countries and pricing named but no separate action step `changelog-20260909-fa2957ab`

WAS THIS USEFUL? 👍 👎

1Password

Feedback ⓘ 5 RELEASES · 2026-09-08 BLOG ↗ RANK

All the latest releases from the 1Password team

> 1Password's biggest change this window is a per-request SSH agent approval prompt shipped identically on Mac and Windows, alongside a public-beta AI Assistant and a Google Calendar offboarding action in SaaS Manager, MDM-configurable browser extension connections on Mac, and smaller password-suggestion and Safari account-creation updates across the app family.

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

01 **Per-request SSH agent approval prompts** NEW 65

Adds a setting under `Settings > Developer > Advanced > 'Ask approval for each new'` that configures the SSH agent to prompt for approval on every SSH request, shipped identically for 1Password for Mac and 1Password for Windows.

Enforce explicit approval for every SSH operation — useful on shared or high-security workstations where unattended agent forwarding is a risk.

> 📍 In 1Password, go to Settings › Developer › Advanced and enable Ask approval for each new.

Require explicit approval for every SSH agent request — useful when you want to audit or control which operations use your SSH key in real time.

> 📍 In 1Password, go to Settings › Developer › Advanced and enable Ask approval for each new.

– Names exact setting path but only UI navigation, no CLI

1Password for Windows 8.12.36 (2026-09-… 1Password for Mac 8.12.36 (2026-09-08)

THINNER COVERAGE BELOW

02 **Google Calendar offboarding workflow action** NEW 45

Adds a workflow action in SaaS Manager to remove all events from a user's primary Google Calendar during offboarding.

– Describes behaviour but no setup steps given 1Password SaaS Manager #1626 (2026-09-0…

03 **MDM-configurable browser extension connections** NEW 45

Enables administrators to configure the 1Password app to connect to the 1Password browser extension in additional browsers through mobile device management (MDM).

– Names MDM mechanism but no config keys or steps `1Password for Mac 8.12.36 (2026-09-08)`

04 **Cross-domain Claude login item suggestions** IMPROVED

45

Extends claude.ai login item suggestions in 1Password for Windows to cover claude.ai, claude.com, and anthropic.com across all three domains.

– Names the three domains but no user-facing action

`1Password for Windows 8.12.36 (2026-09-…`

05 **In-browser 1Password account creation for Safari** NEW

40

Adds the ability to create a 1Password account directly from the 1Password browser extension for Safari.

– Clear capability named but no flow details `1Password in the browser 8.12.36 (2026-…`

06 **AI Assistant in SaaS Manager (public beta)** NEW

30

Adds an AI Assistant to 1Password SaaS Manager in public beta, available by default for new SaaS Manager customers.

– No detail on what the assistant does or how to use it

`1Password SaaS Manager #1626 (2026-09-0…`

07 **Updated password and website requirement suggestions** IMPROVED

25

Updates password generation and change suggestions with new password and website requirements, shown when generating or changing passwords, in 1Password for Windows and 1Password for iOS.

– General claim of new requirements without concrete rules

`1Password for iOS 8.12.36 (2026-09-08)` `1Password for Windows 8.12.36 (2026-09-…`

08 **OIDC custom workflow setup screen layout** IMPROVED

20

Improves the layout of the custom workflow (OIDC) setup screen and workflow entries in 1Password for Windows.

– Layout tweak described with no specifics on what changed

`1Password for Windows 8.12.36 (2026-09-…`

09 **Performance improvements for large vaults** IMPROVED

15

Improves performance when viewing items and browsing large vaults in 1Password for Mac.

– No metrics or scope beyond a general claim `1Password for Mac 8.12.36 (2026-09-08)`

WAS THIS USEFUL? 👍 👎

Auth0 Feedback ⓘ 1 RELEASE · 2026-09-08 BLOG ↗ RANK

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

> Auth0 added a Deny All rule to its Tenant ACL, allowing wholesale blocking of incoming traffic without needing IP or geolocation signal matching.

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

01 **Deny All rule for Tenant ACL** NEW 67

Tenant ACL rules gain a `match_all: true` attribute that creates a Deny All rule, rejecting all incoming traffic to the assigned scope without requiring IP or geolocation signal matching.

.
.
.
.

— Names exact attribute but lacks usage example or scope detail.

New Deny All Rule for Tenant ACL (2026-…

WAS THIS USEFUL? 👍 👎

Clerk

Feedback ⓘ 2 RELEASES · 2026-09-08 → 2026-09-09 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”.

> Clerk shipped OAuth Device Authorization Grant support, enabling CLIs, smart TVs, and other input-constrained devices to authenticate via a standards-based OAuth flow.

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

01 **OAuth Device Authorization Grant flow** NEW 76

Clerk adds the OAuth Device Authorization Grant flow to authenticate CLIs, smart TVs, and other input-constrained devices, supporting both public clients (Client ID only) and confidential clients (Client ID + Client Secret). Clerk's Account Portal serves as the hosted verification page, presenting the OAuth application name, requested scopes, Organization selection, and approve/deny actions to the authorizing user. When enabled and the verification page is reachable, Clerk automatically advertises `device_authorization_endpoint` and grant type `urn:ietf:params:oauth:grant-type:device_code` via OAuth 2.0 and OpenID Connect metadata discovery.

.
.

— Names endpoint, grant type, and client types; no code sample given.

changelog-20260909-8dea503f OAuth Device Authorization Grant (2026-…

WAS THIS USEFUL? 👍 👎

Nudge Security

Feedback ⓘ 1 RELEASE · 2026-09-08 NOTES ↗ RANK

Discover every SaaS and AI asset, harden security posture, and scale identity governance.

> Nudge Security extended its browser extension to Safari, giving companies full SaaS and AI visibility and identity risk detection across every Mac, alongside in-browser nudges to correct risky behavior.

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

01 Safari browser extension for SaaS and AI visibility NEW

70

The Nudge Security browser extension now supports Safari, deployable silently across company Macs via Apple Business Manager and MDM, with step-by-step instructions in Nudge Security settings. It monitors SaaS and AI activity in real time (daily AI usage, logins, access patterns, file uploads), detects identity and access risks (weak or reused passwords, SSO or MFA bypass attempts, shared credentials, risky password manager use), and delivers automated, customizable in-browser nudges to guide employees toward safer behavior.

Roll out the Safari extension silently to all company Macs without requiring employee action, using your existing MDM.

> 📍 In Nudge Security settings, go to the deployment guide for Safari support, follow the step-by-step instructions, and configure silent rollout through Apple Business Manager and your MDM.

— Names deployment method and detection types but only a settings UI path, no API/flag

Deploy the Nudge Security browser exten…

WAS THIS USEFUL? 👍 👎

Ory

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

Ory delivers identity and access management (IAM) for applications, enterprises, and AI agents. Cloud-native, API-first, and self-hostable.

> Ory Hydra now validates OAuth 2.0 client `grant_types` at creation and update time, catching misconfigured clients earlier.

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

01 Grant types validation on OAuth 2.0 clients IMPROVED

48

Ory Hydra now validates the `grant_types` field when creating or updating an OAuth 2.0 client, catching misconfigured clients at registration time.

— Names the field but not error behavior or rejected value list.

Ory Hydra, Ory Polis v26.3.12 released

WAS THIS USEFUL? 👍 👎

ConductorOne

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

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

> ConductorOne's single release this window centers on new agent classifiers that police MCP tool calls for data sensitivity and exfiltration risk, alongside four new session-policy preview API endpoints, MCP resource governance, and two breaking changes to automation expressions and finding field names.

└──▷ **WHAT SHIPPED · 18 FEATURES** most completely described first ? what's the number?

01 **Agent classifiers for MCP tool calls** NEW 75

Agent classifiers evaluate private-data sensitivity, untrusted-content exposure, and exfiltration capability at MCP tool-call time, routing matches to a hook, human approval, or block. A new Observe mode logs what a rule would have caught without denying anything, letting admins test rules safely before enforcement.

— Names mechanism and modes but no config key or API surface changelog-20260909-ec85e1f8

02 **Tenant-wide bulk request limit** NEW 75

Admins can set a tenant-wide bulk request limit (1–100, default 10) from `Governance > Forms`.

Cap the number of entitlements a user can request at once to reduce over-provisioning risk across the tenant.

📍 In the ConductorOne console, go to Governance › Forms, locate Bulk request limit, and set a value between 1 and 100 (default is 10).

— Exact config location, range, and default with runnable steps

changelog-20260909-ec85e1f8

03 **Session policy preview API endpoints** NEW 70

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 covers, including the conferring group.

— Describes endpoint behavior fully but no exact paths given changelog-20260909-ec85e1f8

04 **Expanded system log events and fields** NEW 70

System log events gain a `groups[]` field and `correlation_uid`, plus four new Identity & Access event classes: Account Change, Entity Management, User Access Management, and Group Management.

— Names all fields and event classes verbatim changelog-20260909-ec85e1f8

05 **Bulk and individual finding reprocessing** IMPROVED 70

Findings can now be reprocessed against current transformation/routing rules individually, in bulk, or from a finding's detail view, with the option to keep or reset manual changes.

– Describes modes and options but no exact UI path or API changelog-20260909-ec85e1f8

06 **Automation expressions require explicit step/field paths** 70

BREAKING

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

– Explains migration trigger and required fix clearly changelog-20260909-ec85e1f8

07 **Findings 'Owner' field renamed to 'Assignee'** BREAKING 70

The Owner column, filter, and detail field on findings are renamed to Assignee. API or webhook consumers of the Finding object and audit-log/SIEM pipelines must update to the new field and event names.

– Names affected surfaces and required consumer update changelog-20260909-ec85e1f8

08 **Connector sync failing finding type** NEW 65

A new Connector sync failing finding type fires after two consecutive failed full syncs and auto-resolves on the next successful sync.

– Clear trigger and resolution mechanism, no exact API/UI path

changelog-20260909-ec85e1f8

09 **MCP resource approval and entitlements** NEW 60

A new tab in MCP server management lets admins approve discovered static resources and URI templates; each approved resource receives its own read entitlement.

– Names UI location and entitlement mechanism, no exact path given

changelog-20260909-ec85e1f8

10 **Role mining threshold and enrollment controls** IMPROVED 60

Role mining adds a shared-access threshold control, entitlement list fine-tuning before acting, and optional routing of automatic profile enrollments through an access request task.

— Names three distinct improvements, no exact UI navigation changelog-20260909-ec85e1f8

THINNER COVERAGE BELOW

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

The entitlement binding picker now shows other entitlements from the same app, enabling same-app bindings (e.g. Salesforce Admin → Salesforce Editor).

— Concrete example given but no exact UI path changelog-20260909-ec85e1f8

12 **Stricter SSO silent and passive auth handling** IMPROVED 55

SSO applications now honor OIDC requests for silent or fresh authentication and SAML passive requests, returning an error instead of silently reusing a session when a request cannot be completed safely.

— Names protocols and behavior change, no config surface changelog-20260909-ec85e1f8

13 **Auto-created API credential on device registration** NEW 50

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

— Clear behavior described, no config or limit details changelog-20260909-ec85e1f8

14 **Reorder provisioning steps in place** IMPROVED 50

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

— Clear before/after behavior, no exact UI path changelog-20260909-ec85e1f8

15 **All users toggle in edit owners picker** IMPROVED 50

The Edit owners picker on an app's details page now includes an All users / Owners toggle so admins can see and manage the complete owner list, including suspended users.

— UI path given but no deeper mechanism changelog-20260909-ec85e1f8

16 **Upfront duration limits in request forms** IMPROVED 50

Duration limits for entitlements are now displayed up front in request forms; Indefinite is hidden when a max is set, and invalid existing durations are auto-adjusted.

— Describes behavior and edge case, no exact UI location changelog-20260909-ec85e1f8

17 **Suspended-user flags in access requests** IMPROVED 45

Access-request flows now flag when the target user — or the holder of already granted access — is suspended.

— Behavior described plainly, no mechanism or path changelog-20260909-ec85e1f8

18 **Guided MCP server connection flow** IMPROVED 35

Adds a guided step-by-step flow for connecting MCP servers, replacing the previous single multi-step form.

— Thin UI description, no mechanism or exact steps changelog-20260909-ec85e1f8

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! Automation expressions that reference the bare workflow context — or pass it to a function — no longer compile; each expression must name the step and field directly. Existing running automations 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. API or webhook consumers of the Finding object and audit-log/SIEM pipelines must update to the new field and event names.

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ 8 RELEASES · 2026-09-09 BLOG ↗ RANK

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

> JumpCloud's window is dominated by AI governance infrastructure — a new AI Gateway, MCP Server, and Agent Identities for non-human AI agents — alongside a multi-org Enterprise Portal with centralized Active Directory Integration, GA launches of Custom Admin Roles and Access Risk Detection, and broad expansion of SaaS Management, Password Manager, RADIUS, MFA/SSO, and Windows/Apple/Android device management, plus several breaking API and RBAC scope changes.

└──▷ **WHAT SHIPPED · 52 FEATURES** most completely described first ? what's the number?

01 **MCP Server and MCP discovery in AI Gateway** NEW 90

Adds the JumpCloud MCP Server for Admins, configurable with the AI Gateway to expose management operations to MCP-compatible clients, reaching GA for direct admin interaction via the Model Context Protocol. Adds `MCP Discovery` and `Token & Cost Tracking` under `Access > AI & SaaS Management > Settings > Enhanced Discovery Options` to discover MCP servers and track token usage/cost from Cursor, Claude Code, OpenCode, Codex, and VS Code Copilot CLI; adds an MCP Connection Status column (`Discovered` , `Connected` , `Not Available`) to `Access > AI & SaaS Management > Applications` ; and requires MCP servers in AI Gateway to have a mandatory association with an SSO application or bookmark via the `App` dropdown for group-based scoping.

Expose JumpCloud admin operations to any MCP-compatible AI client (e.g. Cursor, VS Code) through the AI Gateway for governed, auditable admin automation.

> 📍 In the JumpCloud Admin Portal, follow `Configure JumpCloud MCP Server for Admins for the AI Gateway` and `Get Started: JumpCloud MCP Server for Admins` to register the MCP server with your AI Gateway, then connect your MCP client to the gateway endpoint.

Enable MCP server discovery and AI coding tool token cost tracking across managed devices to gain visibility into AI tool usage in your fleet.

> 📍 In the JumpCloud Admin Portal, go to Access › AI & SaaS Management › Settings. Under Enhanced Discovery Options, enable MCP Discovery and Token & Cost Tracking.

— Exact config paths, column values, and requirement named

`Release Notes 2026 (2026-09-09)` `Release Notes 2025 (2026-09-09)`

02 **Systemusers reactivate endpoint migration** BREAKING 90

Removes `GET https://console.jumpcloud.com/systemusers/reactivate/{id}` (now 404) and replaces it with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` carrying `activation_email` in the request body; scripts, automations, and integrations calling the old endpoint must be updated.

Reactivate a user account using the new POST endpoint after the deprecated GET endpoint is removed

```
$ curl -s -X POST
'https://console.jumpcloud.com/systemusers/reactivate/<id>' -H
'x-api-key: <api_key>' -H 'Content-Type: application/json' -d
'{"activation_email": "<email_address>"}'
```

Migrate an automation that reactivates a user account from the deprecated GET endpoint to the new POST endpoint

```
$ curl -s -X POST
'https://console.jumpcloud.com/api/systemusers/reactivate/<user-
id>' \
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json' \
  -d '{"activation_email": "user@example.com"}'
```

— Exact old and new endpoint plus runnable migration example

Release Notes 2024 (2026-09-09)

---

03 **Enterprise-level ADI domain management in Enterprise Portal**

NEW

87

Adds enterprise-level Active Directory Integration domain creation and management via `Enterprise Configuration > Identity Management > Active Directories`; supports sharing ADI domains across sub-organizations through `Configurations > Active Directory`; enables per-user and per-user-group access grants via the `User Group` and `Users` tabs; and supports `Delegated Password Validation` during setup so users can authenticate to the User Portal with existing AD credentials on first login.

Set up a new enterprise-level ADI domain in the EP to centrally manage AD sync across all managed sub-organizations.

📍 1. Log in to the Enterprise Portal (EP). 2. Click `Enterprise Configuration`. 3. In the Left Nav, go to Identity Management › Active Directories. 4. Click `+ Add ADI Domain`. 5. Select 'Manage users and passwords in JumpCloud, AD or both', then click Next. 6. Enter the AD domain name (e.g. `DC=example`; `DC=com`) and click Next. 7. Review userPrincipalName and sAMAccountName attribute mappings, then click Save. 8. Optionally enable `Delegated Password Validation` and download ADI agents.

Share an enterprise ADI domain with specific sub-organizations so they can use the centrally managed AD integration.

📍 1. In the EP, go to the Configurations tab and select the Active Directory pillbox. 2. Click the name of the ADI domain — the Share Configuration aside will appear. 3. Select the secondary organizations to share the domain with. 4. Click Save.

— Exact nav paths plus step-by-step setup and sharing examples product docs

04 **Custom Admin Roles / RBAC scope reorganization and GA**

BREAKING

84

Renames Policy Management to Access Management , System Management to Devices , and Authentication Policies to Conditional Access Policies and IP Lists ; splits Identity Management into a user-only scope, moving Directory Management and Group Management under a new Directory and Groups Management scope; groups SaaS Applications and Asset Management under SaaS and Asset Management ; moves RADIUS Authentication into Access Management ; folds Application Templates into Applications ; consolidates User Portal operations/APIs under Multi-Factor Authentication ; adds CRUD plus No Access permission levels to Identity Management and Application Management scopes; and reaches General Availability enabling granular, responsibility-based role tailoring. Existing custom roles referencing old scope names must be updated.

— Exact old/new scope names given but no migration tooling detail

Roles Based Access Release Notes 2025 (… Release Notes 2025 (2026-09-09)

05 **Password Manager desktop app capacity, region, and management upgrades**

IMPROVED

84

Adds EU region selection on the desktop app activation page and browser extension pairing page; raises item storage to up to 30,000 items without autofill or 13,000 with autofill, and up to 5,000 per shared folder; adds a native ARM build for Apple M1+ macOS with auto-upgrade from x64; paginates items at 100 per page with sorting by nickname and other criteria; adds admin shared-folder management (create/update/view, assign users/groups, manual per-folder sync, Move All button, shared folder events synced to Directory Insights); adds Cloud Backup as a secure fallback; adds an auto-lock schedule (default 15 minutes, up to 1,440 minutes) and an Auto Lock setting tied to device lock; adds item archiving, multi-select, bulk folder deletion, a Copy button in Password History, an import loading indicator, Download Logs / Keyboard Shortcuts settings, and a What's New link; enhances CSV export for the legacy Password Manager to support migration into JumpCloud Vault; and enables admin install/update via command template v2.0.0 without end-user admin permissions after initial run.

Enable EU region support at account activation so that credentials are stored and processed within the EU region.

> 📍 On the Password Manager desktop app activation page, select `EU` as your region before completing account activation. For the browser extension, choose `EU` on the pairing page before pairing.

— Numeric limits and named settings, but scattered across releases

What's New: Password Manager Desktop Ap… | Release Notes 2024 (2026-09-09) | Release Notes 2023 (2026-09-09)

---

06 **AD Integration Agent reliability and sync improvements** IMPROVED

83

Adds single-label domain support in the AD Sync Agent via refactored Root DN validation (domains like `DC=internal` now sync; `jcadimportagent.config.json` uses semicolons e.g. `DC=example;DC=com`); exponential backoff with jitter on the AD Sync Agent connection stream and the AD Import Agent directives stream to reduce LDAP bind floods and reconnection surges; Delegated Authentication mapping changed to use only UPN and `sAMAccountName`; a non-blocking user sync workflow that logs and skips users with attribute errors and retries automatically; case-insensitive `objectGUID` lookups to prevent duplicate-object errors on OU moves/renames; AD password length support expanded to 256 characters; configuration audit logging on startup (excluding secrets); timestamp-first log formatting; password sync from JumpCloud now only triggers on a real change or difference; automatic self-healing connectivity recovering from DC disconnections during routine 10-minute checks; capture of exact AD password-change timestamps for correct ordering; and ADI support for installation on 2022 domain controllers/member servers without workarounds.

— Names config file and fields but no full setup walkthrough product docs

---

07 **Agent Identities for non-human AI agents** NEW

81

Adds Agent Identities to represent non-human AI agents, with Agent Groups and integration with Amazon Bedrock AgentCore, later reaching Public Preview under `Identity Management > Agents` with OAuth-based agent authentication, group-based access control via `Identity Management > Agent Groups`, and MCP server authorization through the AI Gateway.

Issue managed identities to autonomous AI agents (e.g. Amazon Bedrock AgentCore agents) so they appear in access logs and can be governed like human users.

> 📍 In the JumpCloud Admin Portal, go to Agent Identities › Agents › Get Started: Agent Identities, create an agent identity, assign it to an Agent Group, then follow

Integrate Agents with Amazon Bedrock AgentCore to bind the identity to your Bedrock agent.

Register an AI agent identity and scope its SSO application access via groups, so its credentials and permissions are managed independently from human user accounts.

📍 In the JumpCloud Admin Portal: 1. Go to Identity Management › Agents and click + Add. Enter the agent name, owner, and company email on the Details tab. 2. On the Authentication tab, generate OAuth client credentials for the JumpCloud AI Gateway. 3. Go to Identity Management › Agent Groups, create an Agent Group, add the agent, and assign SSO applications to the group.

— Concrete UI paths and OAuth mechanism with worked example

Release Notes 2026 (2026-09-09)

---

08 **JumpCloud Go passwordless login** NEW 81

Adds JumpCloud Go, a hardware-protected, phishing-resistant passwordless browser extension login for managed macOS and Windows devices using Apple Touch ID and Windows Hello; sets it as the default MFA method for Conditional Access Policies on SSO apps, verifying device and user each session; and integrates JumpCloud Go, SAML, or OIDC SSO with AWS Verified Access for VPN-less access to corporate web resources.

Verify that JumpCloud Go is enforced as the default MFA method for an SSO app session — confirm every session triggers device and user verification.

📍 In the Admin Portal, go to SSO Applications › select an app › Conditional Access › confirm MFA method is set to JumpCloud Go, then have a user authenticate via the JumpCloud Go browser extension using Touch ID or Windows Hello.

— Mechanism, default-MFA behavior, and a verification example

Release Notes 2023 (2026-09-09)

---

09 **API filter escaping for pipe characters** IMPROVED 80

Adds support for escaping the `|` (pipe) character with `\` inside `in` and `nin` API filter operators, e.g. `GET /systemusers?filter=department:$in:Finance \| Accounting|IT`, so pipe characters can appear within filter search terms.

Filter system users whose department is Finance | Accounting or IT — now possible because the pipe character can be escaped in API filter search terms

```
$ curl -s -H 'x-api-key: <api_key>'
'https://console.jumpcloud.com/api/systemusers?
filter=department:$in:Finance \| Accounting|IT'
```

Filter systemusers by a department value that itself contains a pipe character, now that `|` can be escaped with `\` in `$in` queries

```
$ curl -s -X GET 'https://console.jumpcloud.com/api/systemusers?
filter=department:$in:Finance \| Accounting|IT' \
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json'
```

— Exact endpoint and escape syntax with runnable curl examples

Release Notes 2024 (2026-09-09)

10 **Windows management policy expansion** NEW 79

Adds six Windows MDM CSP-based policies — Windows Wi-Fi Configuration Policy, Windows VPN Policy, Install Certificate Policy, Bluetooth Configuration Policy, Control Policy Conflict (default on), and Windows Notification Service (default on) — plus a Simple Certificate Enrollment Protocol (SCEP) policy, three Windows Personalization policies (Taskbar Customization, Screen Saver Configuration, Desktop and Lock Screen Settings), and Windows 11 25H2 support across Windows management components.

— Every named policy listed, no per-policy config walkthrough

Release Notes 2025 (2026-09-09) Release Notes 2024 (2026-09-09)

11 **Dynamic Groups filter operator deprecation** DEPRECATED 79

Deprecates the Dynamic Groups `memberQuery` filter operators `$le` and `$ge`, replacing them with `$lte` and `$gte`; existing API scripts using `$le` / `$ge` must be updated (Admin Portal-managed Dynamic Groups are unaffected).

— Exact old/new operator names with clear migration note Release Notes 2024 (2026-09-09)

12 **Custom Query Builder in Insights Reports** NEW 78

Adds a Custom Query Builder under `Insights > Reports` supporting both a manual report builder and AI Assistant natural-language queries, with operators (Equals, Contains, Is Null), CSV/JSON export, and scheduled reports.

— Named operators, formats, and exact UI location Release Notes 2026 (2026-09-09)

13 **RADIUS authentication enhancements** NEW 78

Adds Certificate Based Authentication to RADIUS supporting passwordless X.509-compliant auth from any certificate authority, including imported org-managed certs; adds RADIUS authentication via Azure AD credentials without managing users/passwords outside Azure AD; lets admins add multiple IP addresses to a single RADIUS server configuration; and adds faster EAP reconnect letting recently authenticated devices skip the full handshake using a cached session credential.

Enable passwordless RADIUS access for devices using org-managed X.509 certificates instead of passwords.

> 📍 In the Admin Portal, go to RADIUS › Authentication › Certificate Based Authentication, import your X.509-compliant certificate authority, and assign it to the target RADIUS server.

— Named auth mechanisms with a setup example for cert auth

Release Notes 2025 (2026-09-09) Release Notes 2024 (2026-09-09)

Release Notes 2022 (2026-09-09)

---

14 **Enterprise Portal (Preview) cross-org management suite** NEW

76

Introduces the Enterprise Portal (Preview) as a single pane of glass for administering multiple orgs, adding Google Workspace integration, Google SSO for federated admin auth, Configure Global MFA (Preview) to enforce MFA across all orgs, administrator role management, cross-org MDM device management, cross-org ad hoc commands, cross-org device monitoring and alerting, command template management, SSO application management, policy management, and user/group management.

When onboarding as an enterprise admin managing multiple orgs, start here to set up the Enterprise Portal and enable Google Workspace integration.

> 📍 In the Enterprise Portal (Preview), go to Get Started: Enterprise Portal (Preview), then follow Get Started: Google Workspace Integration in the Enterprise Portal (Preview) to connect your Google Workspace tenant.

Enforce MFA uniformly across all organizations managed through the Enterprise Portal without configuring each org individually.

> 📍 In the Enterprise Portal (Preview), go to Settings › Configure Global MFA (Preview) and enable your required MFA methods to apply them across all managed organizations.

Run a one-off remediation command on a device in any managed organization without switching portals.

> 📍 In the Enterprise Portal (Preview), go to Devices, select the target device, then choose Run Ad Hoc Commands on Devices to execute a saved command template or enter a custom command.

— Many sub-capabilities named but each described in one line product docs

---

15 **AI Gateway for securing AI client connections** NEW

76

Adds AI Gateway to proxy and secure AI client connections, with integrations for Datadog, Vanta, Google Workspace Apps, HubSpot, Apollo.io, Linear, Asana, Slack, GitHub, Cloudflare, GitLab, and Atlassian Rovo, and supports connecting AI clients including Claude, ChatGPT, Gemini CLI, OpenAI Codex, Cursor, VS Code, and Copilot CLI through the Gateway.

Route a developer's Claude session through the AI Gateway so all AI traffic is authenticated and audited via JumpCloud.

> 📍 In the JumpCloud Admin Portal, go to AI Gateway › AI Gateway Integrations, select `Configure AI Gateway Integrations`, then follow `Users: Connect Claude to the AI Gateway` to point the Claude client at your AI Gateway endpoint.

– Long named integration/client list but mechanism stays high-level `product docs`

---

16 **Access Risk Detection (GA)** NEW 76

Introduces Access Risk Detection (GA) providing behavior-based detection of unusual locations, impossible travel, unfamiliar devices, dormant accounts, and abnormal login volumes across the Admin Portal, User Portal, device logins, and SSO applications, with configurable risk factors, automatic MFA-based resolution, and email, Slack, and webhook notifications.

– Detailed detection scope and response mechanism, no setup steps

`Release Notes 2026 (2026-09-09)`

---

17 **Self Service App Catalog** NEW 76

Adds an `App Delivery Method` setting on App Catalog apps with `Auto` and `Self Service` values, enabling a Self Service App Catalog for macOS and Windows so users can install, update, and uninstall apps from the Menu Bar or Tray App without admin intervention.

Make a catalog app self-service so users can install it on demand from the Menu Bar or Tray App without waiting for admin action.

> 📍 In the JumpCloud Admin Portal, go to Software Management › App Catalog, open an app, and set the App Delivery Method to Self Service. Users will see the app in their catalog in the JumpCloud macOS Menu Bar App or Windows Tray App.

– Named setting and values with an activation walkthrough `Release Notes 2026 (2026-09-09)`

---

18 **LDAP security enhancements** IMPROVED 76

Restricts JumpCloud LDAP TLS connections to five modern cipher suites (`TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`, `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`, `TLS_RSA_WITH_AES_128_GCM_SHA256`), removing weak CBC-mode and SHA-1/SHA-256

suites, and adds source IP tracking for incoming LDAP requests for enhanced traceability.

— Exact cipher suite names listed, no client-side action needed

Release Notes 2025 (2026-09-09)

19 **Password Manager Linux build migration off AppImage** BREAKING 75

Discontinues the `.appimage` Linux build as of April 18, 2024; users must migrate to the RPM build (added for x64 Red Hat distributions such as Fedora) or the existing Debian/Ubuntu x86 build, both supporting automatic updates.

— Exact date and named replacement builds for migration

What's New: Password Manager Desktop Ap…

20 **MFA and JumpCloud Protect enhancements** IMPROVED 75

Adds TOTP as an MFA factor for LDAP applications alongside Protect push; adds Push Bombing Mitigation blocking more than one push per resource within sixty seconds, configurable in MFA Configurations; adds Duo Universal Prompt support alongside existing Duo two-factor; splits WebAuthn enrollment into Security Keys and Device Authenticators / Device categories; adds lock-screen push approval/denial via long-press (iOS) or notification expansion (Android); enables MFA by default for new admin accounts; lets admins exclude specific user groups from Protect Push enforcement so they use TOTP only; and lets users reset passwords from the User Portal when MFA is enforced but not yet enrolled.

Enforce TOTP as a second factor for LDAP application access across your org.

📍 In the Admin Portal, go to Directory › LDAP › select your LDAP server › MFA Settings, enable TOTP as an allowed MFA factor, and save.

Enable Push Bombing Mitigation settings — for example to raise the concurrent attempt limit — after a wave of fraudulent MFA push attempts is detected against admin accounts.

📍 In the Admin Portal, go to Security › MFA Configurations, locate the Push Bombing Mitigation section, and adjust the maximum concurrent attempts limit or toggle the protection off.

Protect admin accounts from MFA push bombing by reviewing the default sixty-second lockout window and adjusting maximum concurrent attempts.

📍 In the Admin Portal, go to Security › MFA Configurations › Push Bombing Mitigation › review the sixty-second block period and set Maximum Concurrent Attempts to your desired threshold, or toggle off to disable.

Restrict a user group from Push MFA enforcement so field workers in regions without reliable connectivity can authenticate with TOTP only.

> 📍 In the Admin Portal, go to MFA › JumpCloud Protect › Unified MFA Settings, select the user group to exclude from Push enforcement, and save — members will then authenticate using TOTP instead of Push.

— Several named MFA mechanisms with configuration examples

Release Notes 2025 (2026-09-09) | Release Notes 2023 (2026-09-09) | Release Notes 2022 (2026-09-09)

---

21 **Remote Assist remote desktop support** NEW 74

Launches free JumpCloud Remote Assist remote desktop access on Windows and macOS with no limit on session time or count (requires Agent v1.61.0+, silently installs Remote Assist agent v0.2.4); adds Background Tools with remote command line and remote file transfer, support for the Windows Server initial login screen, user-switching during a session, and a `Ctrl+Alt+Del` shortcut in the Session Options toolbar; and ships Remote Assist as two architecture-specific packages (ARM64 for Apple Silicon, x86_64 for Intel) with automatic binary selection.

Use Remote Assist Background Tools to transfer a diagnostic script to an end-user machine without interrupting the user's active session.

> 📍 In the Admin Portal, open Devices, select the target device, click Remote Assist › Background Tools, then use Remote File Manager to upload the script to the device.

— Version requirements named with a background-tools example

Release Notes 2024 (2026-09-09) | Release Notes 2023 (2026-09-09) | Release Notes 2022 (2026-09-09)

---

22 **Conditional Access Policy enhancements** NEW 73

Adds a disk-encryption device condition (FileVault on macOS, system drive encryption on Windows, root disk encryption on Linux); introduces Monitor Mode for Conditional Access Policies; and enables Device Trust and conditional access for mobile devices managed by third-party MDMs (Jamf, Kandji, Google Workspace EMM) via shared-secret device registration and SSO Extension profile configuration.

Enforce that only encrypted devices can access corporate resources by adding a disk encryption condition to a Conditional Access Policy.

> 📍 In the Admin Portal, go to Security › Conditional Access Policies, create or edit a policy, add a new Device Condition, and select `disk encryption enabled` (FileVault for macOS, system drive encrypted for Windows, root disk encrypted for Linux) as the required condition.

— Named third-party MDMs and mechanism, with a config example

Release Notes 2026 (2026-09-09) Release Notes 2022 (2026-09-09)

23 **Dynamic Groups automation** NEW 73

Launches dynamic group automation for device and user groups with attribute-based membership rules and an optional review step before changes take effect; adds Vendor and Public IP Address attributes for dynamic device group rules and Manager for dynamic user group rules.

Automate device group membership by public IP range so newly enrolled remote endpoints are grouped without manual intervention.

📍 In the Admin Portal, go to Device Groups › Create Group › set Type to Dynamic › add attribute rule: Public IP Address contains '203.0.113.' › save to apply automatically as devices enroll.

— Named attributes with a rule-creation example Release Notes 2023 (2026-09-09)

24 **SaaS Management, Shadow AI, and license tracking** NEW 72

Introduces SaaS Management to discover, categorize, warn, and block shadow-IT SaaS apps via the JumpCloud Go browser extension, with manual app addition and licensing tracking; later removes the JumpCloud Go app requirement so the extension alone suffices for unmanaged-app discovery. Adds a Shadow AI Dashboard in the renamed JumpCloud AI & SaaS Management for visibility into generative AI adoption, usage by department, and most active users, and adds SaaS License Management (GA) for automated license tracking and cost optimization.

— Clear scope and mechanism but no config specifics Release Notes 2025 (2026-09-09) Release Notes 2024 (2026-09-09)

25 **Asset Management enhancements** NEW 72

Adds a dedicated Asset Manager admin role; adds file upload (an Invoice field under Purchase Details) and custom File Upload fields to asset records; adds Disk Size to Hardware Specifications; adds a Local Device Accounts display under Device Management on the Asset Detail page; and adds asset cloning that automatically clears unique fields to prevent duplicates.

— Named fields and role, no navigation steps given Release Notes 2025 (2026-09-09)

26 **Custom REST API Import Connector upgrade** IMPROVED 72

Upgrades the Custom REST API Import Connector for HR-driven provisioning with a custom attribute mapping UI, a transformation expression engine upgrade from GO to

EXPR, flexible sync scheduling (hourly to weekly), and custom API header pairs for vendor-specific security tokens.

– Named engine change and scheduling range, no config example

Release Notes 2026 (2026-09-09)

27 **Directory Insights logging and alerting enhancements** IMPROVED 71

Adds an `sso_auth` event to logs capturing forced re-authentication events; splits the Application Name filter into Application Name, Application Display Name, and Application Display Label, and Resource Name into Resource Name, Resource Display Name, and Resource Display Label; and adds alert trigger conditions based on event frequency to Insights rules so alerts fire only when defined criteria are met.

Audit forced re-authentication events across your SAML/OIDC apps by filtering Directory Insights for the new event type.

📍 In the Admin Portal, go to Directory Insights, add a filter for Event Type = `sso_auth`, and review the resulting log entries to confirm step-up authentication is being triggered for high-stakes applications.

– Named fields and event type with an audit example Release Notes 2026 (2026-09-09)

Release Notes 2025 (2026-09-09)

28 **JumpCloud Go session management** IMPROVED 70

Adds a JumpCloud Go session management section under `User Portal > Security > Multi-Factor Authentication`; logging out of the User Portal no longer terminates an active Go session, and Go sessions now automatically refresh on device login or unlock, removing extra verification challenges.

– Exact portal path and before/after behavior described Release Notes 2024 (2026-09-09)

29 **Access Requests with approval flows** NEW 70

Adds JumpCloud Access Requests with configurable approval flows, webhook integration (e.g. JIRA), and tracking via Directory Insights; later adds the ability to create admin access requests directly from the JumpCloud Menu Bar (Mac) or Windows Tray App without accessing the full User Portal.

Configure an Access Request approval flow and connect it to JIRA so tickets are auto-created when users request elevated access.

📍 In the Admin Portal, go to Access Requests › Configure Approval Flows, create a new flow assigning the appropriate approvers, then under Webhooks add your JIRA endpoint so that each new request automatically opens a JIRA ticket and sends a real-time notification.

— Named webhook use case and a configuration walkthrough Release Notes 2026 (2026-09-09) Release Notes 2025 (2026-09-09)

30 **Multi-Tenant Portal management enhancements** NEW 70

Adds Create Custom Command Templates for MSP admins to reuse commands across tenant organizations; adds an MTP Homepage widget for bulk-exporting available reports (last 24 hours) as JSON or CSV; adds an MDM Certificate & Token Status Board (evolving from an earlier MDM Upcoming Certificate Expirations widget) tracking expiry of MDM, SSO, and AzureAD tokens/certificates with an aggregate MSP view; enables ad hoc commands directly from the Multi-Tenant Portal and Admin Portal; enables adding new users and devices from the MTP with export and bulk-action support; and adds billing visibility for viewing/consuming licenses and downloading the JumpCloud contract.

— Named widgets and export formats across the portal Release Notes 2023 (2026-09-09) Release Notes 2022 (2026-09-09)

31 **Apple MDM policy expansion** NEW 69

Adds GA of BYOD enrollment for iOS/iPadOS 18+ via Account-Driven User Enrollment (ADUE); two MDM policies controlling Apple Intelligence on iOS/iPadOS 18.1 and macOS 15.1 Sequoia; Apple Business Manager as a new service discovery method for Account-driven Enrollment; and updated Mac Personalization policies for Dock Settings and Items and Lock Screen (Screen Saver).

— Named policies and OS versions but no setup steps Release Notes 2025 (2026-09-09) Release Notes 2024 (2026-09-09)

32 **Windows App Catalog auto-update management** NEW 69

Introduces the JumpCloud App Catalog for Windows, supporting auto-update management for 1Password, Adobe Acrobat Reader DC, Chrome, Firefox, Google Drive, OneDrive, OpenVPN, Slack, Webex, and Zoom.

— Full named app list but no configuration steps Release Notes 2024 (2026-09-09)

33 **Global MFA Requirement bulk enforcement** NEW 68

Adds `Account > Settings > Global MFA Requirement` in the Multi-Tenant Portal, letting admins with Billing permission bulk-enforce MFA across all MSP admins from a single setting.

— Exact setting path named, no rollout detail beyond that Release Notes 2024 (2026-09-09)

34 **macOS software update management policies** NEW 68

Adds the ability to schedule or force macOS software updates for individual devices with configurable timeframes and user delay/cancel flexibility; adds macOS Ventura software management policies to delay or block upgrades to macOS 13; and adds a Managed

Login Items policy for macOS 13 to prevent end users disabling persistent software such as the JumpCloud Agent.

Prevent macOS devices from automatically upgrading to Ventura while you validate compatibility across your fleet.

> 📍 In the Admin Portal, go to Device Management › Policies, create a new policy, select `Delay or Block MacOS Ventura`, configure the delay window, and assign it to your macOS device groups.

— Named OS version and policy with a step-by-step example `Release Notes 2022 (2026-09-09)`

---

35 **RSS feed subscriptions for release notes** NEW 68

Adds RSS feed subscriptions for the JumpCloud Help Center via `Subscribe to Support RSS Feed`, `Subscribe to Release Notes and Bug Fixes RSS Feed`, `Subscribe to Agent Release Notes RSS Feed`, and `Subscribe to Bug Fixes RSS Feed`, covering What's New content, product release notes, agent release notes, and bug fix reports.

Subscribe to only JumpCloud agent release notes in your RSS reader to track agent-level changes without noise from other Help Center content.

> 📍 Go to the JumpCloud Release Notes and Bug Fixes page › click `Subscribe to Agent Release Notes RSS Feed` › copy the feed URL into your RSS reader.

— Names all four feed options with a subscribe example

`Subscribe to New Feature and Product Up…`

---

36 **Android device management expansion** NEW 67

Adds full Android 15 support in MDM; Android zero-touch enrollment for fully managed, dedicated, and company-owned devices with a work profile; and support for fully managed and dedicated Android EMM devices including 7 new policies such as Factory Reset Protection, Kiosk Mode, and System Updates, plus general Android EMM enrollment via work profile for company-owned and personal devices.

Enroll a new Android corporate device hands-free using zero-touch enrollment so it arrives fully managed without IT physically handling it.

> 📍 In the Admin Portal, go to Device Management › Android EMM › Zero-Touch Enrollment, generate an enrollment token, and assign it to your zero-touch customer account in the Google zero-touch portal.

— Named policy examples plus a zero-touch enrollment walkthrough

`Release Notes 2024 (2026-09-09)` `Release Notes 2023 (2026-09-09)`

---

37 **SSO protocol and connector additions** NEW 67

Adds OpenID Connect (OIDC) SSO support; adds the Deel SSO Connector; adds a two-screen Identity First Login flow for the User Portal and SSO apps as groundwork for future passwordless/federation; introduces Forced Re-authentication honoring `ForceAuthn="true"` in SAML and `prompt=login` in OIDC; and adds Authentication Methods References (AMR) claims in SAML assertions and OIDC ID tokens to verify the MFA factor used.

– Named protocol parameters but no end-to-end walkthrough Release Notes 2025 (2026-09-09)

Release Notes 2023 (2026-09-09) Release Notes 2022 (2026-09-09)

38 **Device Monitoring and Alerting** NEW 65

Introduces proactive monitoring of device health (availability, software, uptime, disk, battery), policy/command/software management results, directory events such as user addition and privilege elevation, and custom alerts via command execution monitoring across Windows, macOS, and Linux endpoints.

– Broad scope listed but no configuration path given Release Notes 2024 (2026-09-09)

39 **SCIM group management enhancements** IMPROVED 63

Enhances SCIM group management with a dedicated mapping UI supporting name overrides, extended schema mapping, side-by-side object transformation previews, and flexible test data selection for custom activation validation, with all sync activity logged to Directory Insights.

– Describes UI capabilities but no concrete mapping example

Release Notes 2026 (2026-09-09)

40 **Patch management policies and reporting** NEW 62

Adds a universal Google Chrome Browser Patch Management policy keeping Chrome current across macOS, Windows, and Linux from a single policy; adds the Browser Patch Management Policy Report for compliance audits showing devices' current browser versions; and adds the OS Patch Management Policy Report showing which policies apply to each device and their status.

– Named report types but no navigation or filter detail Release Notes 2022 (2026-09-09)

41 **Command execution management enhancements** IMPROVED 62

Adds a Command After Agent Install command type letting admins specify enrollment commands that run immediately after the agent installs on new devices, and adds a Running column to the commands queue to distinguish waiting from actively running commands.

– Named command type and UI column, no full workflow Release Notes 2022 (2026-09-09)

42 **Linux platform support additions** NEW 60

Adds JumpCloud agent support for Linux Fedora 37, and adds a Linux Forbidden Services policy to remove unnecessary or unsupported service types from Linux fleets, reducing attack surface.

Block Linux services that are unnecessary for daily operation to reduce the attack surface across your Linux fleet.

> 📍 In the Admin Portal, go to Device Management › Policies, create a new policy, select `Linux Forbidden Services Policy`, choose the service types to forbid, and apply the policy to the target Linux device group.

— Named OS version and policy with an application example `Release Notes 2022 (2026-09-09)`

43 **Admin Portal and User Portal usability improvements** IMPROVED

60

Adds a `⌘/Ctrl + K` keyboard shortcut in the Admin Portal for quick search and navigation; adds `Password Date` as a viewable column on the Users page; divides the User Portal Applications area into `All Applications` and `Favorites` tabs with application starring and a responsive search field; and changes default password-policy behavior so users comply on their next password change rather than immediately, while retaining a firm compliance date option.

— Several named UI tweaks, each thin on its own `Release Notes 2024 (2026-09-09)` `Release Notes 2023 (2026-09-09)`

THINNER COVERAGE BELOW

44 **Support Case and Customer Portal** NEW

58

Launches the JumpCloud Case Portal centralizing support cases and ideas with filterable search and one-click case detail views; adds Live Chat in the Admin Portal for Premium Support customers with automatic status recognition (no PIN needed); and adds a Customer Portal with sortable columns (Last Modified Date, Account, Requester) plus attachment and ticket-editing support.

— Names UI elements but no workflow specifics `Release Notes 2025 (2026-09-09)` `Release Notes 2022 (2026-09-09)`

45 **SentinelOne integration via Commands** NEW

58

Adds a SentinelOne integration via the JumpCloud Commands feature to download and install the SentinelOne Agent on macOS, Windows, and Linux devices.

— Named integration and platforms, no command syntax given

`Release Notes 2022 (2026-09-09)`

46 **AI Admin Assistant, Commands Builder, and AI Search** NEW

55

Adds AI Admin Assistant for natural-language admin interactions, AI Commands Builder to help admins construct JumpCloud commands (reaching GA for generating Windows, macOS, and Linux commands from plain-English prompts), and JumpCloud AI Search for natural-language search across the admin portal.

– Names three tools but no usage mechanics given Release Notes 2025 (2026-09-09)

47 **Self-Service Account Provisioning** NEW 54

Adds Self-Service Account Provisioning for new users to bind their account to JumpCloud-managed macOS and Windows devices from the login window, including a new macOS login window with wireless connectivity controls.

– Named capability described but no setup steps given Release Notes 2023 (2026-09-09)

48 **JumpCloud Password Manager launch** NEW 54

Adds the JumpCloud Password Manager with end-to-end encrypted local sync, browser extension auto-fill, secure password sharing, and password generation.

– Names core mechanisms but no setup or limits given Release Notes 2022 (2026-09-09)

49 **IPA file support in Private Repository** NEW 44

Adds IPA file support to the JumpCloud Private Repository for deploying iOS and iPadOS app packages.

– Single-line addition with no deployment steps Release Notes 2025 (2026-09-09)

50 **Microsoft 365 integration extended to security groups** IMPROVED 38

Extends the Microsoft 365 integration to include M365/Azure AD security groups.

– One-line extension with no mechanism or setup detail product docs

51 **Service Accounts for APIs** NEW 34

Adds Service Accounts for APIs that are not tied to individual Admin accounts.

– Single-line description with no mechanism or setup detail

Release Notes 2025 (2026-09-09)

52 **Trial recap summary** NEW 26

Adds a trial recap summary giving insight into feature usage during a JumpCloud trial.

– Single generic sentence with no detail on contents Release Notes 2022 (2026-09-09)

└──▷ ALSO FROM THESE RELEASES

Block macOS Ventura upgrades fleet-wide before your org is ready to support the new OS.

> 📍 In the Admin Portal, go to Device Management › Policies › New Policy, select `macOS` and choose the `Delay or Block macOS Ventura` software management policy, then bind it to the target device group.

└──▷ BREAKING ON UPGRADE

- ! The `.appimage` Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.
- ! `GET https://console.jumpcloud.com/systemusers/reactivate/{id}` is removed and now returns a 404; replace with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body.
- ! Dynamic Groups `memberQuery` filter operators `$le` and `$ge` are deprecated and replaced by `$lte` and `$gte`; existing API scripts using `$le` or `$ge` must be updated.
- ! The `Policy Management` scope is renamed to `Access Management` — any custom role referencing the old name must be updated.
- ! The `System Management` scope is renamed to `Devices` — any custom role referencing the old name must be updated.
- ! The `Authentication Policies` scope is renamed to `Conditional Access Policies and IP Lists` — any custom role referencing the old name must be updated.
- ! `Identity Management` no longer bundles directory/group content; `Directory Management` and `Group Management` are now under the separate `Directory and Groups Management` scope — roles relying on the old bundled scope may lose coverage.
- ! `SaaS Applications` and `Asset Management` are now under `SaaS and Asset Management` — roles referencing the old individual scope names must be updated.
- ! `RADIUS Authentication` has moved from its previous location into the `Access Management` scope — roles that granted RADIUS permissions separately must be reconfigured.
- ! `Application Templates` are now part of the `Applications` scope rather than a standalone scope — roles granting only Application Templates access must be reviewed.
- ! User Portal APIs and operations are now enforced under the `Multi-Factor Authentication` scope — roles granting User Portal access without MFA scope permissions may lose access.
- ! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error — replace it with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` in all scripts, automations, and integrations.
- ! The `$le` and `$ge` Dynamic Groups `memberQuery` filter operators are deprecated and replaced by `$lte` and `$gte` — update any API requests using these operators (Admin Portal-managed Dynamic Groups are not affected).
- ! MCP servers previously created in AI Gateway without an associated SSO application or bookmark must now have one assigned — 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.

! The `Policy Management` scope is renamed to `Access Management` — any documentation or automation referencing the old name must be updated.

! The `System Management` scope is renamed to `Devices` — any documentation or automation referencing the old name must be updated.

! The `Authentication Policies` scope is renamed to `Conditional Access Policies and IP Lists` — any documentation or automation referencing the old name must be updated.

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

Cisco Duo Desktop

Feedback ⓘ 1 RELEASE · SEEN 2026-09-09

NOTES ↗ RANK

Cisco Duo secures workforce access and defends against advanced identity threats with IAM, phishing-resistant MFA, SSO, passwordless, and device trust.

> Duo Desktop 7.21 broadens endpoint security product recognition to 13 new vendors, adds a telemetry consent flow with admin controls, and improves device posture signals with virtual environment detection and OS update/agent reporting for Secure Access.

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

01 **Telemetry consent prompt and preference** NEW 68

On first launch after upgrading to 7.21 or later, users see a one-time opt-out notification letting them turn off error and usage data collection and reporting; it does not reappear on later upgrades. The underlying preference is optional and can be set per-user in app preferences or configured system-wide by administrators to bypass the startup prompt entirely.

— Names the prompt behavior and admin/per-user configuration options. snapshot-20260909

THINNER COVERAGE BELOW

02 **13 new endpoint security integrations recognized** NEW 56

Duo Desktop now recognizes 13 additional endpoint security products for device health checks: Check Point Endpoint Security (macOS and Windows), Cynet Endpoint Security (macOS and Windows), ESET Security (Windows), Forcepoint One (macOS and Windows), HarfangLab (macOS), Huntress (macOS and Windows), Nessus (macOS and Windows), Netskope (macOS and Windows), Sophos AV (macOS and Windows), Sophos Home (macOS and Windows), Trend Micro Apex One (macOS and Windows), VMware Carbon Black Cloud, and Xcitium (Windows).

— Lists many named products but no mechanism or config surface. product docs

03 **OS update and agent status reporting for Secure Access** NEW 38

Reports OS automatic update status and management agent detection to Secure Access as additional device health signals.

— Names the signal type but not how it affects access decisions. snapshot-20260909

04 **Virtual environment detection for GCE and Azure** NEW

32

Duo Desktop now detects Google Compute Engine and Microsoft Azure as virtual environments as part of device posture signals.

— States the capability but no detail on how detection is used. snapshot-20260909

WAS THIS USEFUL? 👍 👎

ScoutDNS

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

DNS filtering and threat protection for businesses, MSPs, schools, and nonprofits. Block malware, phishing, and unwanted content at the DNS layer.

> ScoutDNS's Windows Client 2.2.9 adds automatic fallback for internal DNS name resolution, preventing failures on domain-joined machines.

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

01 **Private-name fallback in Windows Client** NEW

67

The Windows Client now falls back to the adapter's private resolvers when queries for suffixes like `.local`, `.corp`, or `.internal` are not covered by any Local Forwarder rule, instead of returning SERVFAIL. This lets AD-joined devices resolve domain controllers and internal hosts without a profile change.

— Clear mechanism and named suffixes, but no config key or flag given.

Windows Client 2.2.9 adds a fallback fo…

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

NoLabs nono

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

RANK

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

> nono's latest updates focus on operational hygiene: a new audit cleanup subcommand with disk-retention filters, finer-grained Unix socket grants for sandboxed commands, and Nix-based installation.

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

01 Audit session cleanup subcommand NEW 88

`nono audit cleanup` prunes old audit sessions from disk, supporting `--keep`, `--older-than`, `--max-total-size <MB>`, and `--dry-run` filters that can be combined to narrow which sessions are removed. `--max-total-size` evicts the oldest sessions until total audit storage falls below the specified megabyte threshold, useful for capping disk usage in CI or shared systems.

Preview which audit sessions would be removed before committing to a cleanup — useful before running in CI or on a shared system.

```
$ nono audit cleanup --keep 10 --max-total-size 500 --dry-run
```

Enforce a rolling retention policy that keeps only sessions from the last 30 days and caps total disk usage at 500 MB, removing oldest sessions first.

```
$ nono audit cleanup --older-than 30 --max-total-size 500
```

Cap audit storage in CI environments where disk is limited — purge oldest sessions to stay under 500 MB without touching recent runs.

```
$ nono audit cleanup --max-total-size 500
```

— Full flag set and commands given, no other mechanism detail v0.76.0

02 unix_socket_bind in tool sandbox profiles NEW 88

Adds `unix_socket_bind` field to `CommandSandboxConfig` in tool-sandbox profiles, allowing per-command Unix domain socket grants (e.g. the Git fsmonitor socket) without

widening the agent-level sandbox. Configured via `command_policies.commands.<cmd>.from.session.sandbox.unix_socket_bind` in the sandbox config JSON.

Grant a sandboxed `git` command access to its fsmonitor socket without giving the agent-level sandbox the same socket bind rights.

```json
{
  "command_policies": {
    "commands": {
      "git": {
        "from": {
          "session": {
            "sandbox": {
              "fs_read": ["."],
              "unix_socket_bind": ["/tmp/git-fsmonitor.sock"]
            }
          }
        }
      }
    }
  }
}
```

— Named config field with example JSON snippet and use case v0.76.0

03 **Nix flake support for installation** NEW 60

Adds Nix flake support, enabling `nix run github:nolabs-ai/nono` and `nix profile add github:nolabs-ai/nono` installs without needing Homebrew or the install script.

— Exact install commands given but no further mechanism v0.76.0

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 9, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue