THE CYBER TOOLCHAIN

NO. 077

# Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 17, 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 189 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 38 tools

▾ // THE BRIEF HIDE

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

Three unrelated things stand out. Endor Labs' Package Firewall now blocks malicious VS Code extensions, closing an install path most SCA looked at. Brinqa collapses duplicate findings from overlapping

vim ? help

scanners into one vulnerability with one owner. Passbolt's beta offline mode lets users unlock and autofill marked credentials when the server is unreachable.

PROTECT

**Stop a malicious package — or IDE extension — before it lands on a developer machine**

Endor Labs extends Package Firewall from registry packages to VS Code extensions, a channel developers install from freely and that rarely appears in any dependency inventory; Threat Center adds tenant-wide monitoring so a newly flagged malicious package surfaces across every repo at once rather than at the next scan. cve-lite-cli's new override-hygiene rule catches the quieter failure — a version override pinned to a floor that is itself vulnerable, which looks remediated in reports.

Endor Labs · cve-lite-cli

PROTECT

**Work one vulnerability instead of five copies of it**

Brinqa's ExploitIQ deduplication merges the same underlying flaw reported by different scanners into a single Intelligent Vulnerability, so counts and SLAs reflect real work rather than tool overlap, and SmartFlows lets teams build the routing for it without code. Sysdig scopes risk acceptances to the scanned asset's OS and CPU platform, so an exception granted for one image variant no longer silently suppresses the finding everywhere else.

Brinqa · Sysdig Secure

PROTECT

**Keep people logged in and authorized when the auth path breaks**

Passbolt's offline mode caches resources users have explicitly marked, so a server outage no longer locks the team out of the credentials they need to fix it — the usual failure mode where the password manager is on the other side of the incident. DNSFilter's macOS roaming client falls back to DNS-over-HTTPS in VPN environments where plain DNS interception fails, and JumpCloud adds forced SAML/OIDC re-authentication for the sessions you want re-proven rather than trusted indefinitely.

Passbolt · DNSFilter

## OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

### OpenOSINT

Feedback ⓘ 1 RELEASE · 2026-09-17 NOTES ↗ RANK

AI-powered OSINT agent with interactive REPL, MCP server, and CLI. 20 tools.

> OpenOSINT v2.29.0 adds Apify cloud actor support, letting the Email Recon tool run entirely in the browser or as an MCP tool without any local installation.

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

01 **Apify cloud actor support for Email Recon** NEW 62

OpenOSINT Email Recon can now run as an Apify cloud actor, from a browser or as an MCP tool in Claude, Cursor, and Windsurf via the Apify MCP Server, requiring no Python, binaries, or API keys installed locally.

— Names the integration and clients but no config/flag detail v2.29.0

WAS THIS USEFUL? 👍 👎

## APPLICATION SECURITY

◆ SAST / SCA / Code Security

# cve-lite-cli

Feedback ⓘ 1 RELEASE · 2026-09-16 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 v1.35.0 adds a new override-hygiene rule to catch vulnerable-floor overrides and expands HTML reports to show all known dependency paths for a finding.

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

01 **Override-hygiene rule OA010** NEW 90

Adds override-hygiene rule `OA010`, which flags an override floor that itself admits a known-vulnerable version — surfacing floors that appear protective but are not. It can be run standalone with `cve-lite /path/to/project overrides` for an override-only audit, or combined with a full scan via `cve-lite /path/to/project --check-overrides` so vulnerable-floor overrides surface alongside CVE findings.

Run an override hygiene audit to catch floors that admit vulnerable versions (OA010) alongside other override problems, without running a full CVE scan.

```
$ cve-lite /path/to/project overrides
```

Include override hygiene (including the new OA010 rule) in a single pass with the regular CVE scan, so vulnerable-floor overrides surface alongside CVE findings.

```
$ cve-lite /path/to/project --check-overrides
```

— Names the rule, its mechanism, and gives runnable commands v1.35.0

THINNER COVERAGE BELOW

02 **Multi-path dependency display in HTML report** IMPROVED 55

The HTML report now shows every known dependency path for a finding, capped at five paths per panel, replacing the previous single-primary-path display.

— Describes the change and its cap but gives no command or path v1.35.0

WAS THIS USEFUL?  

## GitHub

Feedback ⓘ 4 RELEASES · 2026-09-16 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 shipped enterprise-wide bulk SSO authorization for classic PATs and SSH keys, general availability of self-service Copilot budget increase requests, a SCIM profileUrl attribute for user lookups, and broader AI Scan coverage that no longer requires CodeQL default setup.

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

### 01 Copilot budget increase requests reach GA NEW

75

Adds a self-service flow for Copilot users who exhaust their AI credits to request a budget increase, routing requests to the paying account (org or enterprise) for review under Requests from members in Settings > Billing. Organization owners, enterprise owners, and billing managers can approve, adjust, or deny requests by setting a new credit amount, immediately restoring access without leaving settings.

Review and approve a member's Copilot budget increase request as an org owner so they regain AI credit access immediately.

📍 In your organization's Settings, go to Billing › Requests from members, find the pending Copilot budget request, set a new amount, and select Approve and increase.

— Exact UI navigation and approval flow provided Copilot budget increase requests are ge…

### 02 Bulk SSO authorization for classic PATs and SSH keys NEW

70

Adds a new `enterprise_credentials:write` permission for enterprise-installed GitHub Apps enabling credential delegation, plus a new REST API for enterprise credential authorizations that bulk-authorizes a classic PAT or SSH key for up to 50 organizations in a single request, identified by non-secret token ID or SSH key fingerprint. A new enterprise setting lets admins opt in to credential delegation through enterprise-installed GitHub Apps, replacing manual per-organization SSO authorization.

— Names permission and API but not exact endpoint path

Automate SSO authorization for classic …

### 03 profileUrl attribute in SCIM user responses IMPROVED

60

SCIM `/Users` endpoint responses now include a `profileUrl` attribute containing the absolute URL of the linked GitHub account, eliminating extra lookups to match SCIM records to GitHub users. Available across both organization and enterprise SCIM APIs.

— Names field and endpoint but no example call SCIM user responses now include a profi…

THINNER COVERAGE BELOW

04 **AI Scan runs without CodeQL default setup** IMPROVED

40

AI Scan for pull requests now runs on repositories where CodeQL default setup is not configured, broadening security vulnerability detection coverage to eligible repositories without requiring additional setup.

— States before/after but no scope or setup steps

Code scanning AI Scan no longer require…

WAS THIS USEFUL? 👍 👎

## Endor Labs

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

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

> Endor Labs launched Threat Center for real-time, tenant-wide malware and vulnerability monitoring and extended Package Firewall to block malicious VS Code extensions, while also adding malware finding severity classification, Coding Agent Governance MDM deployment with Claude Compliance API support, and background SBOM/VEX exports.

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

01 **Package Firewall for VS Code extensions** NEW 85

Package Firewall now scans every new VS Code extension or update from the Microsoft Marketplace against the policy engine, blocking or warning on malicious extensions and enforcing minimum package age and malware policy before installation and before extensions appear in the marketplace inside the editor; it can be deployed via MDM tools such as Microsoft Intune, Jamf, or Kandji. Documentation now covers each Package Firewall block reason, its meaning, and resolution steps in Understand blocked package responses.

— Names MDM tools and doc page but no exact command

Threat Center and Package Firewall for …

02 **Malware finding severity for potentially affected dependencies**

NEW 85

The Malware finding policy gains a Potentially Affected Finding Severity parameter, letting you raise findings for dependencies whose version constraints could resolve to a malicious package version even when the currently resolved version is clean. Malware findings are now classified as Definitely Affected or Potentially Affected based on how precisely a dependency matches a known malicious package version.

Raise findings for dependencies whose version constraints could resolve to a malicious package — catching exposure before the bad version is actually pinned.

> 📍 In the Endor Labs console, go to Malware finding policy › configure Potentially Affected Finding Severity to your desired severity level (e.g. High), then save the policy.

— Exact config parameter plus console steps to configure it product docs

03 **Coding Agent Governance MDM deployment and Compliance API integration**

NEW

80

Deploy Coding Agent Governance with MDM support enables generation of Cursor hooks, Claude Code settings, Codex requirements, GitHub Copilot policy hooks, or a macOS configuration profile for managed developer machines. Connect the Anthropic Compliance API integration enrolls a Claude Enterprise directory so Coding Agent Governance can match Claude Code sessions to organization roles and groups.

— Names exact config surfaces but no runnable command shown product docs

04 **Ask Permission policy behavior changed for Codex** BREAKING

75

Coding Agent Governance policies with the Ask Permission action in Codex now let the tool call proceed and record the match under Policy Violations as Ask, rather than denying the call outright; Block policies continue to deny. Any policy relied on to stop calls in Codex must be changed to Block.

— Clear before/after behavior and required migration action product docs

05 **Threat Center dashboard for malware and threat monitoring**

NEW

70

Threat Center is a tenant-wide dashboard tracking newly discovered malware, open-source packages, vulnerabilities, and AI models, showing which monitored projects may be exposed before risk surfaces in project-level scans. It gives a real-time view of malicious packages landing on public registries such as npm and PyPI, with impact mapping showing which of your projects pull in an affected package, malware behavior details, and alerts regardless of whether you are impacted; entries also include research write-ups, blog links, and ongoing updates as a campaign develops.

— Explains scope and mechanism but no navigation path given

Threat Center and Package Firewall for …

THINNER COVERAGE BELOW

06 **Background SBOM and VEX export jobs** IMPROVED

50

SBOM and VEX exports now run as background jobs so large projects can export without the request timing out; exports are available per project, finding, or package version.

— Describes mechanism but no command or endpoint named product docs

└──▷ **BREAKING ON UPGRADE**

! Coding Agent Governance Ask Permission policies in Codex no longer block tool calls — calls now proceed instead of being denied. Any policy you relied on to stop calls in Codex must be changed to Block.

WAS THIS USEFUL?

## JFrog

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

JFrog provides DevOps platform for software delivery, managing artifacts, dependencies, and continuous integration/deployment pipelines.

> JFrog Artifactory adds native LuaRocks repository support, letting teams host, proxy, and cache Lua packages for NGINX, OpenResty, and Kong directly from Artifactory.

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

01 **LuaRocks repository type in Artifactory** NEW 78

Artifactory adds LuaRocks as a native repository type supporting local, remote, and virtual repository tiers for Lua packages (rocks and rockspecs). The remote repository type proxies and caches luarocks.org rocks on first request so later pulls are served from Artifactory instead of the public registry; the local repository type stores private first-party rocks, internal libraries, and custom Kong plugins as versioned `.rock` files; and the virtual repository unifies local and remote LuaRocks repositories behind a single endpoint. The `luarocks` CLI can point at an Artifactory virtual repository URL as its registry, replacing direct luarocks.org access for OpenResty and Kong fleets.

— Names repo tiers, file format, and CLI integration but no exact commands

JFrog Artifactory Supports LuaRocks Hos…

WAS THIS USEFUL?

# Checkmarx KICS

Feedback ⓘ 1 RELEASE · 2026-09-17 NOTES ↗

CODE ↗ RANK

Find security vulnerabilities, compliance issues, and infrastructure misconfigurations early in the development cycle of your infrastructure-as-code with KICS by Checkmarx.

> KICS v2.2.0 adds new Terraform and ARM queries to detect disabled Synapse managed virtual network isolation, and removes the `--disable-full-descriptions` CLI flag.

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

01 **Synapse managed virtual network queries** NEW 75

New Synapse Workspace Managed Virtual Network Not Enabled queries detect when managed virtual network isolation is disabled, covering Terraform via the `azurerm_synapse_workspace` resource's `managed_virtual_network_enabled` field and Azure Resource Manager via the `Microsoft.Synapse/workspaces` resource's `managedVirtualResource` field.

— Names exact resources and fields for both platforms. v2.2.0

02 **Removal of --disable-full-descriptions flag** BREAKING 60

The `--disable-full-descriptions` CLI flag has been removed along with the `pkg/descriptions` package it backed; any scan command or script that passes this flag will now fail.

— Names exact flag and package removed, with impact. v2.2.0

└──▷ **BREAKING ON UPGRADE**

! The `--disable-full-descriptions` flag has been removed; any scan command or script that passes this flag will now fail.

WAS THIS USEFUL? 👍 👎

# Veracode

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

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

> Veracode's window centers on deeper CI/CD workflow control — new `veracode.yml` keys for predependency commands, agent pools and analysis branches — plus platform-managed installation and scan scheduling for GitHub and Azure DevOps integrations, alongside IDE plugin refinements, API pagination, an Apex scan noise reduction, and two upcoming deprecations.

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

## 01 New veracode.yml config keys for CI workflow integrations

NEW 90

Adds support for custom predependency commands in the Veracode YAML file to prepare projects before scanning (GitHub Workflow Integration v2.1.3). Adds a custom agent pool name parameter in `veracode.yml` to specify the agent pool for pipeline execution (Azure DevOps Workflow Integration v2.4.3). Adds `analysis_branch` support in `veracode.yml` so scheduled scans run for the specified analysis branch instead of the default branch (Azure DevOps Workflow Integration v2.3.10).

Run scheduled scans against a long-lived analysis branch rather than the repository default branch in Azure DevOps.

```yaml
analysis_branch: release/2026-q3
```

— Names exact config keys, versions, and includes a runnable YAML example.

Integration updates (2026-09-16)

## 02 Pagination support in Platform APIs IMPROVED

80

Adds page size support to the Platform Applications API ( `/appsec/v1/applications` ) for efficient retrieval of large application lists, and introduces support for the Veracode Platform paginated Sandbox REST API for retrieving sandbox lists using pagination (Java API Wrapper v26.3.19.0).

— Names the endpoint and wrapper version but no request/response example.

Integration updates (2026-09-16)

## 03 Platform-managed GitHub and Azure DevOps integration management

NEW 75

Enables installation and configuration of the Veracode GitHub Integration directly from the Veracode Platform, eliminating manual GitHub Marketplace steps, plus a new uninstallation workflow to remove the Veracode app from GitHub organizations. Enables scheduling of Static Analysis, SCA, and Infrastructure as Code (IaC) scans for GitHub organizations directly from the Platform, and scheduling scans for every organization where the Azure DevOps Workflow Integration is installed, based on `veracode.yml` configurations.

— Describes scope of install/uninstall/scheduling flows without exact UI path.

Integration updates (2026-09-16)

---

04 **VeracodeFlawImporter task replaces Veracode Flaw Importer**

DEPRECATED

70

The Veracode Flaw Importer task (with spaces in the name) is deprecated and replaced by `VeracodeFlawImporter` in Veracode Azure DevOps extension v3.35.0; the deprecated task is scheduled for removal in a future release.

— Names exact task identifiers and version, giving a clear migration action.

Integration updates (2026-09-16)

---

05 **Findings filtering and grouping in VS Code extension** NEW

60

Adds a Current File filter to Static Scan Findings in Veracode Scan for VS Code, allowing you to view findings only for the file currently open in the editor, plus an option to filter and group Static Scan Findings by file name, with findings for each file grouped by severity.

— Names the UI filter but only a starting point, not a command.

Integration updates (2026-09-16)

---

06 **End of support for Jira 9.x integration** DEPRECATED

60

Veracode will end support for the Veracode Integration for Jira on Jira Server and Jira Data Center 9.x on November 30, 2026; upgrade to Jira 10 or later to remain supported.

— Gives an exact deadline and required upgrade path. Integration updates (2026-09-16)

THINNER COVERAGE BELOW

---

07 **New platform version support for Jira and Visual Studio** NEW

55

Adds support for Jira 11, including required Java 21 and platform compatibility updates (Veracode Integration for Jira Server v5.0.2), and adds support for Visual Studio 2026 in Veracode Scan for Visual Studio v0.7.2.

— Names versions and requirements but no setup steps. Integration updates (2026-09-16)

08 **Scan Scope setting in Visual Studio extension** NEW

50

Adds a Scan Scope setting in Veracode Scan for Visual Studio to scan the full project directory or only the active solution for faster, more focused results.

— Names the setting and its two modes but no exact navigation.

Integration updates (2026-09-16)

---

09 **Usage analytics added across IDE plugins** NEW

45

Adds usage analytics to provide insights into plugin adoption, feature usage, and scan activity in Veracode Scan for JetBrains v1.8.0, Veracode Scan for Visual Studio v0.8.0, and Veracode Scan for VS Code v1.16.0.

— Names three plugin versions but no user-facing action. Integration updates (2026-09-16)

---

10 **Skips @isTest methods in Apex scans** IMPROVED

40

Static Analysis now skips `@isTest` methods during Apex scans to reduce noise and improve result quality.

— Describes the change but no mechanism detail or metrics.

Static Analysis updates (2026-09-16)

---

11 **Region switching during OAuth in VS Code** NEW

35

Adds an option to change the region during OAuth authentication in Veracode Scan for VS Code, displaying the current or most recently used region.

— Brief description with no further mechanism or steps. Integration updates (2026-09-16)

---

12 **GitHub Fix for SCA** NEW

20

Veracode integrations gain GitHub Fix for SCA.

— Named only in the release summary with no further detail.

Integration updates (2026-09-16)

## └──▷ ALSO FROM THESE RELEASES

. . . .

## └──▷ BREAKING ON UPGRADE

! The Veracode Flaw Importer task (which contains spaces in the task name) is deprecated and replaced by `VeracodeFlawImporter` in Veracode Azure DevOps extension v3.35.0; the deprecated task is scheduled for removal in a future release.

! Veracode will end support for the Veracode Integration for Jira on Jira Server and Jira Data Center 9.x on November 30, 2026; upgrade to Jira 10 or later to remain supported.

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

## infisical

Feedback ⓘ 1 RELEASE · 2026-09-16 NOTES ↗ RANK

Infisical is the open-source platform for secrets, certificates, and privileged access management.

> Infisical restored Oracle Database support in PAM, extended external KMS to AWS US ISO/ISOB regions, and added certificate audit log details to PKI.

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

01 **AWS US ISO and ISOB regions for external KMS** NEW 45

External KMS key management now supports AWS US ISO and ISOB regions.

— Names specific regions but lacks setup detail v0.165.12

02 **Oracle Database support restored in PAM** IMPROVED 25

Oracle Database PAM support, which had been removed, is restored in this release.

— Names the account type but no mechanism given v0.165.12

03 **Certificate audit log details for PKI** NEW 25

Adds audit log details for PKI certificate events.

— Bare description, no fields or endpoint named v0.165.12

WAS THIS USEFUL? 👍 👎

# Truffle Security trufflehog

Feedback ⓘ

1 RELEASE · 2026-09-16 | NOTES ↗ | CODE ↗ | RANK

trufflehog discovers, classifies, and validates leaked credentials

> TruffleHog v3.97.5 adds two new credential detectors, S3 object-level scan filtering, a flag to override ignore-comment suppression, low-memory Git scanning, and an optional detector interface for verification outside the cache.

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

01 **`--no-ignore-tag` flag overrides ignore comments** NEW

75

Adds a `--no-ignore-tag` global flag to report secrets even when the source line carries a `trufflehog:ignore` comment, overriding the usual suppression behavior.

– Exact flag name and clear override behavior stated v3.97.5

02 **Optional GitHub App installationId for org scans** IMPROVED

70

Makes the GitHub App `installationId` optional when scanning all installations, so org-wide scans no longer require a specific installation to be specified.

– Names exact field and before/after behavior change v3.97.5

THINNER COVERAGE BELOW

03 **S3 object filtering for scans** NEW

55

Adds object filtering in S3 scanning, enabling scans to target specific objects within a bucket rather than the entire contents.

– Describes behavior but no exact flag or config key given v3.97.5

04 **New Humio and Resend detectors** NEW

45

Adds the `HumioAPIToken` detector to classify and validate leaked Humio API tokens, and a Resend detector to classify and validate leaked Resend API keys.

– Names both detectors but no scan mechanism detail v3.97.5

05 **Optional detector interface for uncached verification** NEW

45

Introduces a new optional detector interface allowing credentials to be verified even when they are not present in the verification cache.

– Explains mechanism but no interface name or usage path v3.97.5

06 **Low-memory Git scanning mode** NEW 35

Introduces a low-memory Git scanning mode to reduce peak memory usage when scanning large repositories.

— States purpose but no flag name or numbers given v3.97.5

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

## Wallarm

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

Discover the latest features, improvements, and updates in Wallarm API Security

> Wallarm redesigned its WAF Rules interface into a unified, filterable panel with inline rule-path visibility, in-list management, and a guided rule builder.

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

### 01 Redesigned WAF Rules interface with unified panel and builder

NEW 83

The WAF rules interface now shows a unified panel listing every rule type in one view, with each filtered view carrying its own bookmarkable URL. Each rule row displays the full request-targeting path inline (e.g. `HEADER › AUTHORIZATION › JWT › jwt_header › BASE64 › JSON › alg`) without opening the rule, and rows expose endpoint, application, and last-updated metadata. New application and scope filters distinguish `Default` (Wallarm-managed, read-only) rules from team-created rules and persist in the address bar across reloads, so a filtered view can be shared via URL. Rules can be enabled/disabled, duplicated, and deleted directly from the list view, and a new step-by-step rule builder constrains each step to valid options (e.g. Cookie → JWT → Base64 → JSON → sub).

Share a filtered rules view scoped to a specific application with a teammate so they can review coverage without navigating the tree.

> 📍 In the Wallarm dashboard, go to WAF Rules, apply the application filter for your target app and set the scope filter to show only team-created rules (excluding `Default`), then copy the URL from the address bar and send it — the recipient lands on the same filtered list.

— Names filters, URL persistence and rule-path example but no API/config keys.

Introducing the New WAF Rules Interface…

WAS THIS USEFUL? 👍 👎

## REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

# Unfurl

Feedback ⓘ 1 RELEASE · 2026-09-16 NOTES ↗ CODE ↗ RANK

Extract and Visualize Data from URLs using Unfurl

> Unfurl v2026.09 adds a wave of new URL and token parsers — Gmail, Microsoft Defender Safe Links, Facebook, Instagram, GitHub, Fernet, itsdangerous, defanged IOCs and more — alongside Tree/Text views with dark mode in the web UI and a new layered configuration system, while renaming the API key environment variables in a breaking change.

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

## 01 Layered configuration with env vars and local overlay NEW

91

Adds `UNFURL_REMOTE_LOOKUPS` environment variable to enable or disable remote lookups from the environment, overriding both config files. Adds `unfurl.local.ini` as a gitignored, user-local config overlay that overrides `unfurl.ini` without risking committed secrets. Configuration is now layered: Unfurl reads `unfurl.ini`, then `unfurl.local.ini`, then `UNFURL_*` environment variables, then CLI flags, with each layer overriding the last.

Store your VirusTotal key and enable remote lookups in a gitignored local config so they apply to every run without touching the tracked `unfurl.ini`.

ini

```
[UNFURL_APP]
remote_lookups = true

[API_KEYS]
virustotal = <your key>
```

— Exact config keys, file names and a runnable example v2026.09

## 02 Microsoft Defender Safe Links parser NEW

88

New parser extracts the wrapped destination URL from Microsoft Defender Safe Links and decodes the pipe-delimited `data` field (format versions 01 through 05) into recipient, message and tenant GUIDs, a timestamp, scan verdict, and scan payload.

Unfurl a Safe Links-wrapped URL from a phishing email to recover the original destination, recipient GUID, and scan verdict without sending data to external services.

```
$ unfurl 'https://nam12.safelinks.protection.outlook.com/?
url=https%3A%2F%2Fevil.example.com%2Fpayload&data=05%7Crecipient-
guid%7C...'
```

— Names field format versions and a runnable command v2026.09

03 **API key environment variables renamed** BREAKING 85

The old bare lowercase API key environment variable names ( `bitly` , `virustotal` , `google_kg` ) are deprecated and now log a warning; they must be renamed to `UNFURL_BITLY_API_KEY` , `UNFURL_VIRUSTOTAL_API_KEY` , and `UNFURL_GOOGLE_KG_API_KEY` .

— Clear before/after names for required migration v2026.09

04 **Defanged indicator refanging parser** NEW 80

New parser recognizes defanged indicators (e.g. `hxxps://evil[.]com/payload[.]exe` , `1.2.3[.]4` , `user[at]evil.com` ) and refangs them into a new node, with a hover listing every replacement made.

Refang a defanged IOC from a threat report and extract all embedded structure in one step.

```
$ unfurl 'hxxps://evil[.]example[.]com/payload[.]exe'
```

— Concrete examples and a runnable command v2026.09

05 **Fernet token parser** NEW 68

New parser extracts the version, cleartext creation timestamp, IV, ciphertext, and HMAC from Fernet tokens, including the re-padded form used by ChatGPT Ads click IDs ( `oppref` , `olref` ).

— Names fields and a specific click-ID use case v2026.09

06 **Facebook URL and fbclid parser** NEW 68

New parser covers Facebook URL paths (posts, photos, videos, groups, events, stories, pages, Marketplace, profiles, comments) and decodes modern `fbclid` values into browser ID, app ID, ad ID, and AEM hash.

— Enumerates path types and decoded fbclid fields v2026.09

07 **Gmail URL token parser** NEW 65

New parser decodes Gmail legacy hex and new-style (2018+) URL tokens into Gmail message IDs and embedded timestamps, handling the `th`, `compose`, `permmsgid`, `permthid`, and `projector` URL parameters.

— Names parameters and decoded outputs v2026.09

08 **Unit tests shipped with package** NEW 65

Tests now ship with the package, enabling validation of an installed copy via `python -m unittest discover -s unfurl.tests.unit`.

— Gives an exact runnable command v2026.09

09 **Expanded timestamp and UUID version support** IMPROVED 62

Adds UUID version 6, 7, and 8 support, with timestamps extracted from v6 and v7. Adds new timestamp formats for WebKit milliseconds, Epoch nanoseconds, PostgreSQL, and Mac Absolute Time nanoseconds. Epoch seconds auto-detection now covers dates from 2010 onward, previously 2015.

— Names formats and gives a before/after date v2026.09

10 **YAML-based site definitions system** NEW 62

Adds a YAML-based site definitions system (see `unfurl/parsers/site_defs/README.md`) that lets Unfurl learn a site's URL structure without writing Python.

— Points to the config file that enables it v2026.09

11 **Instagram URL parser** NEW 62

New parser covers Instagram posts, reels, stories, highlights, and profiles, decoding shortcodes and story IDs into creation timestamp, shard ID, and sequence number.

— Explains decoded structure but no example v2026.09

12 **itsdangerous token parser** NEW 60

New parser for `itsdangerous` signed tokens, used by Flask and other Python web apps, extracts the payload (decompressed if needed), the signing timestamp, and the signature.

— Names mechanism but no usage example v2026.09

THINNER COVERAGE BELOW

13 **Google ad click URL parsing** NEW 56

Adds Google `/aclk` ad click URL parsing with parameters `adurl`, `ai`, `gclid`, `sig`, and more, defined via `google.yaml`.

– Names parameters and the defining file v2026.09

14 **Bing form code and image search parameter parsing** NEW 54

Adds Bing `form` code parsing, including indexed variants, and image search parameters (`thid`, `mediaurl`, `sbifnm`, `iss`, `view`, and more).

– Names specific Bing parameters, no example given v2026.09

15 **Additional URL fragment and delimiter parsing** NEW 53

Unfurl now parses Text Fragments (`#:~:text=`) and SPA-style fragment routes (`#/route?key=value`), as well as `;`-delimited `key=value` pairs in URLs as used by ad servers and path parameters.

– Names exact syntax patterns handled v2026.09

16 **GitHub URL parser** NEW 53

New parser covers GitHub URLs for repos, commits, issues, PRs, branches, releases, Actions runs, compare views, OAuth flows, and line-number fragments.

– Broad list of URL types but no mechanism detail v2026.09

17 **Tree and Text views with dark mode** NEW 47

Adds Tree and Text views alongside the Graph view in the web UI, with copy-to-clipboard support for the text tree, and adds dark mode with the user's preference remembered.

– UI addition described without navigation detail v2026.09

18 **40 additional shortener domains supported** IMPROVED 45

Adds 40 more shortener domains including `aka.ms`, `flic.kr`, `redd.it`, `pin.it`, `t.cn`, and `wa.link`, plus Constant Contact click-tracking links.

– Lists sample domains but no mechanism v2026.09

19 **Improved Discord snowflake decoding** IMPROVED 45

Discord snowflakes created after July 2022 are now decoded in general Discord URL paths, and snowflakes in query values and token payloads on Discord domains are also decoded.

— Gives date scope but no example v2026.09

20 **New parsers for MongoDB ObjectIDs, Base32, and Base58** NEW

38

Adds a parser for MongoDB ObjectIDs and their embedded timestamps, plus new parsers for Base32 and Base58 encoding.

— Thin one-line additions grouped as a set v2026.09

21 **File extension type parser** NEW

32

New parser identifies file type from a URL's file extension and flags extensions commonly abused to deliver malware.

— Bare description with no named extensions or mechanism v2026.09

└──▷ **BREAKING ON UPGRADE**

! The old bare lowercase API key environment variable names ( `bitly` , `virustotal` , `google_kg` ) are deprecated and log a warning — rename them to `UNFURL_BITLY_API_KEY` , `UNFURL_VIRUSTOTAL_API_KEY` , and `UNFURL_GOOGLE_KG_API_KEY` .

WAS THIS USEFUL? 👍 👎

## NETWORK SECURITY

◆ Firewalls & Network Defense

## Sophos Switch

Feedback ⓘ 1 RELEASE · 2026-09-16 NOTES ↗ RANK

Sophos Switch is a network orchestration platform enabling centralized management and security policy enforcement across switching infrastructure.

> Sophos Switch Central 2026.41 adds switch-name search to management pages, making it easier to locate devices by name rather than identifier alone.

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

01 **Name-based search on management pages** IMPROVED 45

The search box on switch, site, and stack management pages now supports name-based search, in addition to the existing search criteria.

— Names UI surfaces affected but no further mechanism given

Central 2026.41NewReleased on September…

WAS THIS USEFUL? 👍 👎

## CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

# Sysdig Secure

Feedback ⓘ 1 RELEASE · 2026-09-17 CHANGELOG ↗

RANK

Sysdig Secure is a container security platform providing runtime threat detection, forensics, and compliance monitoring for cloud-native environments.

> Sysdig Secure refined risk-acceptance scoping in the CLI Scanner to match the scanned asset's OS/CPU platform, and the CLI Scanner gained flags for detecting unrecognized executables and summarizing image licenses.

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

## 01 Unknown executable detection flag in CLI Scanner NEW

70

The `sysdig-cli-scanner --detect-unknown-executables <image>` flag scans a container image for vulnerabilities, including binaries not tracked by any package manager, and flags unrecognized executables.

Scan a container image for vulnerabilities including binaries not tracked by any package manager, and flag unrecognized executables too.

```
$ sysdig-cli-scanner --detect-unknown-executables <image>
```

— Runnable command given but no output detail. changelog-20260917-8dcb964b

## 02 License summary flag in CLI Scanner NEW

70

The `sysdig-cli-scanner --show-licenses <image>` flag returns a quick summary of the ten most common licenses found in an image, useful for a fast compliance spot-check in CI.

Get a quick license summary for the ten most common licenses found in an image — useful for a fast compliance spot-check in CI.

```
$ sysdig-cli-scanner --show-licenses <image>
```

— Runnable command given, limit of ten licenses noted. changelog-20260917-8dcb964b

THINNER COVERAGE BELOW

## 03 OS/CPU-scoped risk acceptances in CLI Scanner IMPROVED

50

Risk acceptances scoped to an operating system or CPU architecture are now evaluated against the scanned asset's platform in the CLI Scanner, so an acceptance only applies when the image matches the specified platform.

— Prose description only, no flag or command shown. `changelog-20260917-8dcb964b`

## └──▷ ALSO FROM THESE RELEASES

.
.
.

---

WAS THIS USEFUL?  

◆ CNAPP

# Plerion

Feedback ⓘ 1 RELEASE · 2026-09-17 NOTES ↗ RANK

Plerion is a cloud security platform that discovers and manages vulnerabilities and misconfigurations across infrastructure.

> Plerion renamed custom reports to custom dashboards and added a homepage-assignment action, a drag-and-drop widget builder, and a per-user override for the assigned homepage.

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

## 01 Custom dashboards renamed with homepage assignment NEW

75

Custom reports are renamed to custom dashboards, and a new Assign as homepage action in `Settings > Custom dashboards` lets admins designate a dashboard as the landing page for selected users and user groups on sign-in.

Assign a custom dashboard as the default landing page for a user group so they see role-specific findings on sign-in.

📍 In the console, go to Settings › Custom dashboards, open the dashboard you want to set as the landing page, click Assign as homepage, then select the target users or user groups and confirm.

— Exact settings path and action named, with worked example.

Custom reports are now custom dashboard…

## 02 Per-user home dashboard override NEW

75

A new `Profile > Home dashboard` setting lets individual users override any admin-assigned homepage dashboard; clearing the selection restores the admin-assigned dashboard.

Override an admin-assigned homepage with a personal dashboard so your preferred view loads on every sign-in.

📍 In the console, go to Profile › Home dashboard, select your preferred dashboard from the list, and save. Clear the selection at any time to revert to the admin-assigned dashboard.

— Exact setting path, override, and restore behavior with example.

Custom reports are now custom dashboard…

## 03 Widget builder for custom dashboards NEW

65

A new `Add widget` panel provides ready-made widgets, and a `Build your own` flow lets users construct custom widgets using the `Show me` , `Broken down by` , and `Shown as` fields.

— Named fields given but no navigation path or example.

`Custom reports are now custom dashboard…`

---

WAS THIS USEFUL? 👍 👎

---

## DETECTION & RESPONSE

◆ Security Data Pipeline

# Cribl Stream

Feedback ⓘ 1 RELEASE · 2026-09-17 DOCS ↗ BLOG ↗

RANK

Cribl Stream is a data processing platform that routes, transforms, and enriches data from multiple sources to destinations in real-time.

> Cribl Stream's 4.20 release brings backend functions to Cribl Apps (now GA) and adds AWS Cloud Connections recommendations to speed up source onboarding.

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

01 **Backend functions in Cribl Apps** NEW 75

Adds an `onRequest` handler model to Cribl Apps, letting developers expose app-specific HTTP endpoints that run server-side logic without a user session active. Also adds scheduled function support, enabling recurring background jobs such as periodically pulling from a threat feed, updating a Stream lookup table, and making the latest entries available to a pipeline for enrichment.

— Names the onRequest handler and gives concrete job examples, no exact syntax.

2026-09-17-ffa9e715

02 **AWS Cloud Connections source recommendations** NEW 60

Adds AWS Cloud Connections recommendations in Cribl Stream, which suggests a ranked list of AWS log sources to onboard, Source configuration values, and a Destination from those available in the Worker Group.

— Describes what it suggests but not exact UI steps. 2026-09-17-ffa9e715

THINNER COVERAGE BELOW

03 **Cribl Apps general availability** NEW 30

Promotes Cribl Apps to general availability, making them a supported foundation for building and deploying custom applications on Cribl Stream.

— Status change only, no mechanism or usage detail given. 2026-09-17-ffa9e715

WAS THIS USEFUL? 👍 👎

# Cribl

Feedback ⓘ 1 RELEASE · 2026-09-17 DOCS ↗ BLOG ↗ RANK

Cribl is built for IT and Security data and provides a unified data management platform for exploring, collecting, processing, and accessing that data at scale.

> Cribl this window added backend server-side logic and persistent storage for Cribl Apps, an embedded MCP server for AI-client integration with Cribl.Cloud, alert-muting rules in Cribl Insights, and a new Guard Privacy 3.0 model family for sensitive-data detection.

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

01 **Embedded MCP server in Cribl.Cloud** NEW 75

An embedded MCP server lets external MCP clients (such as Cursor, Claude Code, or Codex) connect to a Cribl environment and interact with Sources, Destinations, Pipelines, metrics, and Search Notebooks through natural language. An admin enables it and copies a Bearer token from `Settings > Global > Information`.

— Names UI path, token flow, and supported clients precisely. 2026-09-17-f002e365

THINNER COVERAGE BELOW

02 **Muting Rules for Cribl Insights alerts** NEW 55

Muting Rules in Cribl Insights allow teams to suppress outbound notifications for matching alerts during a configured time window, created by navigating to Muting Rules and specifying match criteria and a time window.

Suppress noisy alert notifications during a maintenance window by creating a Muting Rule in Cribl Insights.

> 📍 In Cribl Insights, navigate to Muting Rules and create a new rule specifying the matching alert criteria and the time window during which outbound notifications should be suppressed.

— Clear UI steps to create a rule, but no API/config key named. 2026-09-17-f002e365

03 **Cribl Guard Privacy 3.0 model family** NEW 55

Cribl Guard adds the Privacy 3.0 model family for background sensitive-data detection, introducing per-entity detection thresholds and a new Pro model alongside the existing Fast and Base models.

— Names model tiers and thresholds but no usage steps. 2026-09-17-f002e365

04 **Allowed-hosts and SSRF protections in Cribl Apps** NEW 55

Cribl Apps enforces a declared allowed-hosts list at the project root for outbound access, with SSRF protections applied; administrators can authorize additional hosts after install.

— Names the config surface and admin action, no exact file path. 2026-09-17-f002e365

05 **Backend functions for Cribl Apps** NEW 50

Cribl Apps now supports backend functions — server-side logic declared in an App that Cribl deploys and runs alongside it, enabling scheduled work and other operations that should not run in the browser.

:

— Explains mechanism but no concrete config or command given. 2026-09-17-f002e365

06 **KV store for Cribl Apps** NEW 40

Cribl Apps now supports a KV store accessible to App code and backend functions for persistent key-value storage within an App.

— Names the surface but gives no API or limits. 2026-09-17-f002e365

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

# Huntress

Feedback ⓘ 3 RELEASES · SEEN 2026-09-17 NOTES ↗ RANK

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

> Huntress shipped new macOS threat detections for Gatekeeper bypass techniques, extended endpoint visibility to macOS with last-logged-in-user tracking, and added granular scan controls to Managed Antivirus.

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

## 01 Network and Archive File Scanning toggles in Managed Antivirus

NEW 75

Adds two configurable Microsoft Defender scan toggles in Managed Antivirus, both accessible at EDR → Managed Antivirus → Defender Configuration → Scans: Network File Scanning (off by default) and Archive File Scanning (on by default, covers ZIP, RAR, and similar formats).

Enable Network File Scanning for endpoints where mapped network drive coverage is required, such as file servers accessed by a small number of endpoints.

> 📍 In the Huntress console, go to EDR → Managed Antivirus → Defender Configuration → Scans, then toggle Network File Scanning on.

Disable Archive File Scanning for high-throughput endpoints where ZIP/RAR scanning overhead is a concern, while keeping all other Defender defaults intact.

> 📍 In the Huntress console, go to EDR → Managed Antivirus → Defender Configuration → Scans, then toggle Archive File Scanning off.

— Exact UI path and default states given for both toggles.

New MAV Configuration Settings: Network…

## 02 macOS Gatekeeper bypass detection via quarantine stripping

NEW 73

Adds three detections for macOS Gatekeeper bypass: quarantine attribute removal from files in malware staging folders by a script or shell (the ClickFix and AMOS dropper pattern), quarantine attribute removal from files on mounted disk images (used by fake installers), and a combined sequence of a fake installer mount plus quarantine strip on the same machine within five minutes as a high-confidence pre-execution signal. Detection monitors the underlying system call directly rather than the `xattr`

command, so it fires regardless of whether the attacker uses a shell script or compiled binary, and each alert surfaces the file path, attribute removed, and responsible process. Filters out Apple backup and file-sharing services, which accounted for approximately 99% of noise during testing; requires Agent `v0.14.196` or later.

— Detailed mechanism and named techniques, but no user-facing action to take.

Huntress now detects macOS Gatekeeper b…

---

03 **Last logged-in user visible for macOS endpoints** IMPROVED

60

Extends the last logged-in user field on the agent overview page to macOS endpoints, previously Windows-only. Shows the most recent interactive console/GUI login, excluding system-owned login windows and shutdown records; requires Agent `v0.14.196` or later.

During triage or asset review, quickly attribute a macOS host to an individual user without querying the endpoint directly.

> 📍 In the Huntress console, go to the agent overview page for a macOS endpoint and check the `Last Logged In User` field — visible once the endpoint checks in on Agent v0.14.196 or later.

— Clear behaviour and exact UI location, no numeric limits given.

Last logged in user now visible for mac…

---

WAS THIS USEFUL? 👍 👎

## Automox

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

Check out our full list of release notes, and stay up to date with what

> Automox added support for macOS 27 (Golden Gate), verified with Agent 2.6.53.

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

01 **macOS 27 (Golden Gate) support** NEW 30

Automox now supports macOS 27 (Golden Gate), verified with Agent `2.6.53`.

— Names OS version and agent version but no further mechanism.

New Automox Supported Operating System …

WAS THIS USEFUL? 👍 👎

◆ **SIEM**

## Exabeam

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

Exabeam is a security analytics platform that detects insider threats and advanced cyberattacks through behavioral analysis and machine learning.

> Exabeam's Threat Center adds a new API endpoint for retrieving full case lifecycle history and audit events.

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

01 **Case lifecycle history endpoint in Threat Center** NEW 70

A new `GET` API endpoint under `Threat Center > Cases > Get case lifecycle history` retrieves the comprehensive lifecycle history, stage transitions, and audit events of a case.

— Names exact endpoint path but no request/response detail

New Threat Center Endpoint (2026-09-16)

WAS THIS USEFUL? 👍 👎

# Databricks

Feedback ⓘ 4 RELEASES · 2026-09-14 → 2026-09-16 BLOG ↗

RANK

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

> Databricks reached GA on the Unity Gateway API for model and MCP service management across Terraform, CLI and four language SDKs, and previewed upcoming changes including automatic change data feed, compliance-profile JAR tasks on serverless, and a new SQL window function.

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

01 **Unity Gateway API and developer tools GA** NEW 85

The Unity Gateway API for managing model services, model-provider services, and MCP services is now generally available with full create, read, update, list, and delete support. It can be managed via Terraform provider `1.132.0`+, Databricks CLI `v1.17.0`+ (including Declarative Automation Bundles support in Beta), Python SDK `databricks-sdk 0.136.0`+, Go SDK `databricks-sdk-go v0.178.0`+, Java SDK `databricks-sdk-java 0.153.0`+, and JavaScript SDK `@databricks/sdk-aigateway 0.19.0`+.

— Names exact SDK/CLI/Terraform versions but no usage walkthrough

Unity Gateway API and developer tools a…

02 **Automatic Change Data Feed coming to all regions** NEW 65

Automatic Change Data Feed (Auto CDF) will compute row-level changes at query time using row tracking, eliminating the need to enable change data feed on each individual Delta Lake or Apache Iceberg v3 table. It requires Databricks Runtime 19 or above with row tracking enabled on the table, and is rolling out through October 2026.

⋮

— Explains mechanism and runtime requirement but not yet available

Automatic change data feed will soon be…

03 **counter_diff SQL window function** NEW 65

Adds the `counter_diff` analytic window function to Databricks SQL and Databricks Runtime 19+, calculating differences between consecutive cumulative counter values and handling counter resets in time-series analysis.

— Names the exact function and runtime version, no example query given

The counter_diff SQL window function is…

THINNER COVERAGE BELOW

## 04 JAR tasks on serverless for compliance security profile NEW

45

JAR tasks (Java or Scala Spark code) in Lakeflow Jobs will soon run on serverless compute for workspaces with the compliance security profile enabled, removing the need to provision or manage clusters.

— Describes scope and benefit but is an upcoming preview, not yet usable

JAR tasks on serverless compute will so…

WAS THIS USEFUL?  

◆ Threat Intelligence

# Hudson Rock

Feedback ⓘ 1 RELEASE · SEEN 2026-09-17 NOTES ↗ RANK

Hudson Rock is a cybersecurity threat intelligence platform that detects compromised credentials and leaked data across the internet.

> Hudson Rock's Cavalier API gains a Supply Chain Risks view for third-party infostealer exposure, company and account management with a company search endpoint, and six new search endpoints and fields covering term, PC-name, advanced, subdomain and directory-tree queries.

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

## 01 New search endpoints and fields in Cavalier API NEW

75

Adds six new search capabilities to the Cavalier API: a Search by Term endpoint for free-text querying across infostealer records, a Search by PC Name endpoint to look up infostealer-compromised machines by hostname, an Advanced Search endpoint for compound, multi-criteria infostealer queries, a Search Data Field extending query filtering options across existing search surfaces, a Subdomain Filtering feature to scope company and domain searches to specific subdomains, and a Directory Tree field exposing filesystem path data from infostealer-collected machine telemetry.

— Six named surfaces but no HTTP methods or paths given. snapshot-20260917

## 02 Company and account management and search NEW

65

Adds Company Management functionality for organising and administering monitored companies, an Account Management endpoint for programmatic control of account resources, and a Company Search endpoint for querying companies within the Cavalier dataset.

— Endpoints named but no HTTP method or path given. snapshot-20260917

THINNER COVERAGE BELOW

## 03 Supply Chain Risks in Cavalier API NEW

45

Adds a Supply Chain Risks capability that surfaces infostealer exposure across third-party vendor relationships.

— Describes purpose but names no endpoint or method. snapshot-20260917

WAS THIS USEFUL? 👍 👎

# MISP

Feedback ⓘ 1 RELEASE · 2026-09-17 NOTES ↗ RANK

MISP (core software) - Open Source Threat Intelligence and Sharing Platform

> MISP v2.5.47 introduces an AI-assisted analysis integration, native PostgreSQL support, and a new ledger-based database migration system, alongside detection-rule sharing objects, Overmind UI filtering improvements, and updated threat-intel galaxies.

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

## 01 Ledger-based database migration system

BREAKING — 95

Migrates database schema management from a single `db_version` integer to a `schema_migrations` ledger under `app/Lib/Migration/Migrations/`, with pending and failed migrations exposed as `migrations_pending` and `migrations_failed` fields in the diagnostic payload. Adds `cake Admin migrationStatus`, `cake Admin migrationApply` (with `--dry-run` to preview SQL), and `cake Admin migrationCreate` console commands. Fleet monitoring that alerted on `actual_db_version` differing from `expected_db_version` must move to the new fields since `db_version` is now frozen at 159; `runUpdates` (and site-admin login) now stops on the first migration failure instead of continuing.

Check which database migrations are pending or failed before or after an upgrade, to verify schema state across a fleet.

```
$ cake Admin migrationStatus
```

Preview the exact SQL a pending migration will execute without applying it, useful for change-control review before touching production.

```
$ cake Admin migrationApply --dry-run
```

— Runnable commands, named fields, and explicit breaking behaviour. v2.5.47

## 02 AI-assisted analysis integration

NEW — 90

Adds `Plugin.AI_*` settings under a new `AI` tab in server settings, gated by the new `perm_ai_tools` role permission, to configure an AI-assisted analysis integration via the `ai_connector` misp-module. Supports four actions — summarise event, summarise report, recommend tags, and extract indicators — with all AI-derived content tagged with `ai-computer-assisted` provenance tags; adds two workflow action modules, `Summarise report with AI` and `Extract indicators with AI`, and documents the

integration contract in `docs/dev/ai_integration.md`, including a fake module server for testing without an LLM. This replaces the earlier CTIInfoExtractor endpoint and its settings, which are removed.

Enable AI-assisted analysis for analysts by configuring the LLM endpoint and granting the required role permission via the AI tab in server settings.

> 📍 In MISP, go to Administration › Server Settings & Maintenance › AI, set the `Plugin.AI_*` values for your LLM endpoint and model, then use the Test LLM button to verify connectivity. Grant the `perm_ai_tools` permission to the relevant roles under Administration › Roles.

— Names settings, permission, actions, and replaced endpoint with setup steps. v2.5.47

---

03 **PostgreSQL 16 install support** NEW — 65

Adds `INSTALL/POSTGRESQL.sql` and a `PostgresObserverExtended` datasource to support fresh installs on PostgreSQL 16, with install steps documented in `docs/CONFIG.postgresql.md`.

— Names install script, datasource, and docs path. v2.5.47

---

04 **Overmind UI filtering and editing improvements** IMPROVED — 65

Adds a new More filters expandable section to the users, servers, organisations, workflows, logs, galaxy clusters, collections, and event attribute indexes in Overmind. Adds a collection card and *add to collection* action to the event view, a JSON field component used by the decaying model modal, an add button on the event reports tab, and an improved markdown editor for event report previews.

— Names each UI surface but only general navigation. v2.5.47

THINNER COVERAGE BELOW

---

05 **Detection rule sharing objects** NEW — 55

Adds `elastic-detection-rule`, `kql-analytics-rule`, `kunai-rule`, and `splunk-rule` MISP objects for detection rule sharing.

— Names four new object types but no usage example. v2.5.47

---

06 **Threat intel galaxy updates** IMPROVED — 55

Adds a new MITRE ATLAS Case Study galaxy and updates MITRE ATLAS to the 2026.08 release, adds MITRE D3FEND techniques and relations, and moves the MITRE Fraud Framework (F3) to version 1.1 with relationships in misp-galaxy.

— Names specific galaxy versions but no usage steps. v2.5.47

07 **Case-insensitive tag name deduplication** BREAKING 55

Tag names that collide under a new case-insensitive collation on `tags.name` are merged into the oldest tag, with every reference repointed; instances with such collisions will have tags merged automatically on upgrade.

— Explains mechanism and upgrade impact, no manual action needed. v2.5.47

08 **New default feeds: TweetFeed and Threatbase** NEW 35

Adds TweetFeed and several Threatbase feeds to the default MISP feed list.

— Names feed sources but no count or config detail. v2.5.47

09 **Phar stream wrapper hardening** IMPROVED 35

Unregisters the `phar` stream wrapper in both entry points as a defence-in-depth hardening measure.

— Names mechanism but no further operational detail. v2.5.47

└──▷ **BREAKING ON UPGRADE**

! Fleet monitoring that alerted on `actual_db_version` differing from `expected_db_version` must move to the new `migrations_pending` and `migrations_failed` diagnostic fields; the version pair can no longer diverge as the `db_version` counter is frozen at 159.

! `runUpdates` (and site-admin login) now stops on the first migration failure instead of marking the failure as done and continuing.

! The earlier CTIInfoExtractor endpoint and its settings are removed and replaced by the new `Plugin.AI_*` AI integration.

! Tag names that collide under the new case-insensitive collation on `tags.name` are merged into the oldest tag, with every reference repointed — instances with such collisions will have tags merged automatically on upgrade.

WAS THIS USEFUL? 👍 👎

## EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

# Brinqa

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

Brinqa is a risk and security analytics platform that aggregates and correlates security data to prioritize vulnerabilities and threats.

> Brinqa 12.3.295 introduces Vulnerability Deduplication (ExploitIQ) to consolidate duplicate findings into unified Intelligent Vulnerabilities, a no-code SmartFlows automation builder, an expanded public API with matching MCP tools, and scheduled PDF dashboard reporting, alongside BQL query enhancements, connector schema-change review, and a redesigned sidebar.

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

01 **Vulnerability Deduplication (ExploitIQ)** NEW 90

Introduces Vulnerability Deduplication (ExploitIQ), which consolidates duplicate vulnerability definitions into a single Intelligent Vulnerability (IV) and Intelligent Vulnerability Definition (IVD) with consolidated evidence and risk scoring. Adds a deduplication configuration page to turn deduplication on or off, choose participating integration sources, set matching confidence level, and enable or disable individual pipeline steps. Adds a new Intelligent Vulnerabilities relationship tab on Host, Container, and Container Image detail views. Introduces a system-managed SmartFlow and a dedicated trigger deduplication processing action for orchestrating deduplication after data load, plus in-product progress indicators for IV/IVD generation and operational metrics and a dashboard for the deduplication pipeline.

— Explains mechanism, configuration, UI, and orchestration in detail. 12.3.295

02 **BQL query language enhancements** NEW 78

Adds a BQL grammar reference endpoint and a debugging option on the BQL API to inspect generated queries; adds `UNION ALL` support in BQL to combine multiple filter criteria in a single Metric; adds string-literal output columns in BQL, including within unions; and introduces a consolidate-by-BQL action that re-consolidates a selected subset of source records by targeting them with a BQL query.

Use UNION ALL in a BQL Metric to surface critical findings from two separate filter criteria in one query result.

```
$ SELECT id, title, severity FROM findings WHERE severity =
'CRITICAL'
UNION ALL
SELECT id, title, severity FROM findings WHERE cvssScore >= 9.0
```

— Names endpoint and syntax with a runnable example query. 12.3.295

03 **Scheduled PDF Dashboard Snapshots** NEW 76

Introduces Scheduled PDF Dashboard Snapshots: schedule exports as PDFs, target ownership groups, manage a personal My Snapshots inbox with expiration and bulk delete, and deliver via secure link or attachment.

— Names inbox, delivery methods, and lifecycle controls. 12.3.295

04 **Public API and MCP tools expansion** NEW 71

Introduces new public API endpoints and matching MCP tools covering flow execution and history, record comments (create, list, search), dataset writes (single and bulk create/update/delete), button-flow discovery and triggering, and ticket creation from findings. Adds a consolidated Record Comments API supporting read, search, and manage operations, with BQL support for querying comments and traversing them back to their records.

— Lists many endpoint areas but no exact paths given. 12.3.295

05 **Connector Schema Change Review** NEW 71

Adds Connector Schema Change Review: select a connector version, review detected schema changes in a diff table, and Review, Ignore, or Resolve each change inline — with user-customized consolidation mappings preserved across upgrades.

— Describes a clear inline review workflow and preservation behavior. 12.3.295

06 **SmartFlows no-code automation builder** NEW 68

Introduces SmartFlows, a visual no-code automation builder supporting webhook and API triggers, filter and action blocks, parallel orchestration, Email/Slack/Microsoft Teams notifications, and dashboard snapshot delivery.

— Names triggers and channels but no build-step walkthrough. 12.3.295

THINNER COVERAGE BELOW

07 **BrinqaIQ Assistant capability parity** IMPROVED 54

Adds BrinqaIQ Assistant multi-turn context, BQL and CVE lookup grounding, automation launch and tracking, and capability parity with the Brinqa MCP tool surface.

— Lists new abilities without a usage example. 12.3.295

08 **Reusable Notification Templates** NEW 52

Adds Notification Templates with a merge-fields editor, data-model-aware dynamic variables, and the ability to clone and reuse templates across notification actions.

— Describes editor and variables but no config location. 12.3.295

09 **Redesigned sidebar navigation** IMPROVED 44

Redesigns the sidebar with collapsed-rail flyouts, collapsible submenu sections that remember their state, expanded multi-theme support, and broad styling improvements.

— Lists UI changes without exact navigation detail. 12.3.295

WAS THIS USEFUL? 👍 👎

## IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

### Cisco Duo Desktop

Feedback ⓘ 1 RELEASE · SEEN 2026-09-17

NOTES ↗ RANK

Cisco Duo secures workforce access and defends against advanced identity threats with IAM, phishing-resistant MFA, SSO, passwordless, and device trust.

> Cisco Duo Desktop now lets administrators pre-configure the telemetry consent setting org-wide, removing the start-up prompt end users would otherwise see.

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

01 **Admin-configurable telemetry consent preference** NEW 55

A new system-wide administrator preference lets organizations pre-configure the telemetry/error-and-usage-data collection setting for Duo Desktop before deployment. Admins set this via the app's administrator preference controls to enable or disable data collection, bypassing the start-up consent prompt end users would otherwise see.

When deploying Duo Desktop org-wide, pre-configure the telemetry preference so users are never prompted at start-up.

📍 In the Duo Desktop admin configuration, set the telemetry/error-and-usage-data preference system-wide via the app's administrator preference controls to either enable or disable collection before users launch the app.

— Names the setting and admin path but no exact config key or file. snapshot-20260917

WAS THIS USEFUL? 👍 👎

# DNSFilter

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

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

> DNSFilter's macOS Roaming Client v2.4.6 Beta adds a DNS-over-HTTPS fallback for VPN environments and rolls out an updated certificate bundle including a new root CA.

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

01 **DNS-over-HTTPS fallback over VPN** NEW 75

An install-time flag `ENABLE_DOH_FALLBACK=true` maintains DNSFilter enforcement over DNS-over-HTTPS when a corporate VPN blocks the DNS-over-TLS port.

— Names exact flag and trigger condition, no deployment steps

09/16 September 16 – macOS Roaming Clie…

02 **Updated macOS certificate profile with new root CA** IMPROVED 65

Updated macOS certificate profiles now bundle all DNSFilter roots — including the new DNSFilter Root CA G1 — in a single push profile, replacing prior installs in place. Deploy via Deployments → Roaming Clients → Beta Channel, re-download the macOS certificate profile, and push it through MDM to replace the existing profile automatically.

Deploy the updated certificate profile (with DNSFilter Root CA G1 included) to managed Macs via MDM to replace the previously installed profile in place.

> 📍 In the dashboard, go to Deployments → Roaming Clients → Beta Channel, re-download the macOS certificate profile, and push it through your MDM — it replaces the existing profile automatically.

— Names new root CA and gives exact MDM deployment path

09/16 September 16 – macOS Roaming Clie…

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

# BeyondTrust

Feedback ⓘ 1 RELEASE · 2026-09-16 BLOG ↗ RANK

BeyondTrust provides privileged access management and endpoint security solutions to control, monitor, and audit user access to critical systems.

> BeyondTrust's Endpoint Credential Manager 1.6.2609 adds four new appSettings keys covering certificate validation, credential result limits, and plugin debugging, and documents every key ECM reads in Example.config.

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

01 **Certificate revocation validation setting** NEW 80

Adds `requireCertificateRevocationCheck` appSettings key (default `false`) to reject certificates whose revocation status cannot be determined, intended for hosts without a reachable CRL or OCSP endpoint.

Allow ECM to connect when the appliance certificate is issued by an internal CA (e.g. ADCS) that does not publish a CRL — use only until the issuing CA certificate is deployed to the host.

xml

```
<appSettings>
  <add key="requireCertificateRevocationCheck" value="false" />
  <add key="allowUntrustedApplianceCertificate" value="true" />
</appSettings>
```

— Names key, default, and exact use case with runnable config

Endpoint Credential Manager 1.6.2609 re…

02 **Untrusted appliance certificate acceptance setting** NEW 80

Adds `allowUntrustedApplianceCertificate` appSettings key (default `false`) to accept appliance certificates that do not chain to a trusted root, for hosts where the issuing CA is not yet installed.

Allow ECM to connect when the appliance certificate is issued by an internal CA (e.g. ADCS) that does not publish a CRL — use only until the issuing CA certificate is deployed to the host.

```xml
<appSettings>
  <add key="requireCertificateRevocationCheck" value="false" />
  <add key="allowUntrustedApplianceCertificate" value="true" />
</appSettings>
```

— Names key, default, and exact use case with runnable config

Endpoint Credential Manager 1.6.2609 re…

03 **Verbose plugin exception debugging setting** NEW 80

Adds `VerbosePluginExceptions` appSettings key to return full plugin exception text to the appliance for field debugging, replacing the default correlation-ID-only response.

Enable full plugin exception detail during a field debugging session to diagnose credential retrieval failures without a rebuild.

```xml
<appSettings>
  <add key="VerbosePluginExceptions" value="true" />
  <add key="MaxReturnedCredentials" value="750" />
</appSettings>
```

— Names key, default behavior, and debugging use case

Endpoint Credential Manager 1.6.2609 re…

04 **Credential result limit override** NEW 75

Adds `MaxReturnedCredentials` appSettings key to override the credential result limit in configuration, raising the ceiling to 750, without requiring a rebuild.

Enable full plugin exception detail during a field debugging session to diagnose credential retrieval failures without a rebuild.

```xml
<appSettings>
  <add key="VerbosePluginExceptions" value="true" />
  <add key="MaxReturnedCredentials" value="750" />
</appSettings>
```

— Names key and new limit with runnable config example

Endpoint Credential Manager 1.6.2609 re…

THINNER COVERAGE BELOW

05 **Documented appSettings keys in Example.config** IMPROVED

ECM now documents every appSettings key it reads in `Example.config`.

— Names file but gives no further mechanism or scope

Endpoint Credential Manager 1.6.2609 re…

---

WAS THIS USEFUL? 👍 👎

## Auth0

Feedback ⓘ 2 RELEASES · 2026-09-16 BLOG ↗ RANK

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

> Auth0's new B2B Connect Early Access release adds real-time enterprise connection event streaming, automatic IdP-driven session termination, and the ability to connect directly to Auth0 without an external authorization server.

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

01 **Enterprise connection event streaming** NEW 76

Auth0 now streams enterprise connection lifecycle events — `connection.created`, `connection.updated`, and `connection.deleted` — for enterprise connections including Azure AD, ADFS, Google Workspace, Active Directory, LDAP, and Ping, eliminating the need to poll the Management API for connection changes. Events are delivered as CloudEvents-formatted JSON to a webhook, Amazon EventBridge, or a custom event pipeline.

— Names event types, IdPs, and delivery mechanisms but no endpoint

Enterprise Connection Events — Early Ac… | B2B Connect - Enterprise in Early Acces…

THINNER COVERAGE BELOW

02 **Direct Auth0 connections without external IdP** NEW 43

Supports connecting an application directly to Auth0 without an external authorization server, with new quickstart guides provided to get started.

— Mentions quickstart guides as a starting point but no commands

B2B Connect - Enterprise in Early Acces…

03 **Automatic session termination on IdP logout** NEW 38

Automatically terminates active application sessions when the enterprise IdP ends the corresponding session, keeping app and IdP session state in sync.

— Describes behavior but no configuration surface named

B2B Connect - Enterprise in Early Acces…

04 **Email-domain based SSO resolution** NEW 13

B2B Connect Early Access adds email-domain SSO resolution, though the release notes give no further detail on how it works.

— Named only in the summary with no mechanism described

B2B Connect - Enterprise in Early Acces…

└──▷ **ALSO FROM THESE RELEASES**

- 
- 
- 
- 

---

WAS THIS USEFUL? 👍 👎

## JumpCloud

Feedback ⓘ 7 RELEASES · 2026-09-17 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 biggest window additions are a new Access Requests approval workflow with webhook notifications, an MCP Server capability in AI Gateway with usage dashboards and discovery, and forced SAML/OIDC re-authentication support, alongside a wide set of MDM, MFA, SaaS Management and Password Manager improvements plus two breaking API and package changes.

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

### 01 User reactivation API endpoint change BREAKING 84

The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; it is replaced by `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with an `activation_email` field in the request body for user reactivation.

Migrate a user-reactivation integration from the deprecated GET endpoint to the required POST endpoint.

```
$ curl -s -X POST
'https://console.jumpcloud.com/systemusers/reactivate/<user-id>'
\
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json' \
  -d '{"activation_email": "<email_address>"}'
```

— Exact old/new endpoints, method and field, with runnable example

Release Notes 2024 (2026-09-17)

### 02 Forced re-authentication for SAML and OIDC NEW 80

The IdP now honors `ForceAuthn="true"` in SAML and `prompt=login` in OpenID Connect, triggering fresh credential prompts even during active sessions; a new `sso_auth` event in Directory Insights logs captures these forced re-authentication events for both SAML and OIDC sessions.

Audit forced re-authentication events in Directory Insights to verify that high-stakes app step-up logins are being recorded for compliance.

📍 In the Admin Portal, go to Directory Insights, open the Events filter, and select

the `sso_auth` event type to view all forced re-authentication events.

— Exact parameter names and audit event, with UI filter path

Release Notes 2025 (2026-09-17)

---

03 **OAuth client authentication type for agents** NEW 78

Adds a `client authentication type` setting on an agent's Authentication tab, letting admins choose Client secret basic (credentials sent in the authorization header, the default) or Client secret post (credentials sent in the request body) when the agent requests an OAuth token from JumpCloud — matching external platforms such as Amazon Bedrock AgentCore that require a specific credential-delivery method.

Match an external platform's OAuth requirement (e.g., Amazon Bedrock AgentCore) by selecting how the agent sends its client credentials when requesting a token.

📍 In the JumpCloud Admin Portal, open the agent's Authentication tab, then under client authentication type select Client secret basic (credentials in authorization header) or Client secret post (credentials in request body) to match the external platform's OAuth configuration.

Register a new AI agent and configure it to use Client secret post authentication to integrate with Amazon Bedrock AgentCore.

📍 1. Go to Identity Management › Agents and click + Add. 2. Enter the agent name, owner, and company email on the Details tab. 3. On the Authentication tab, generate OAuth client credentials, then set the client authentication type to Client secret post so credentials are sent in the request body.

— Names exact field values and OAuth mechanism via UI path

Release Notes 2026 (2026-09-17)

---

04 **MCP Server monitoring and discovery in AI Gateway** NEW 73

Introduces an MCP Server capability in AI Gateway. Adds a Dashboard tab with org-wide MCP server usage metrics, tool call volume, error rates, trend charts, and per-server drill-down; MCP servers already running on managed devices can be discovered and connected via Access > AI & SaaS Management > Applications, checking the MCP Connection column for Discovered status and clicking Add MCP Server.

Discover and connect an MCP server already running on a managed device to AI Gateway without leaving the SaaS management view.

📍 1. Go to Access › AI & SaaS Management › Applications. 2. Find the application and check the MCP Connection column for Discovered. 3. Click the status, review

the discovered MCP servers, then click Add MCP Server to connect it to AI Gateway.

— Names dashboard metrics and exact discovery UI path Release Notes 2026 (2026-09-17) Release Notes 2025 (2026-09-17)

05 **Password Manager Linux package migration** BREAKING 67

The Password Manager Linux `.appimage` build is discontinued (unsupported as of April 18, 2024) and replaced by RPM and Debian (Ubuntu x86) packages; existing `.appimage` users must delete their current build and download the new package from the Password Manager downloads page.

— Exact deprecation date and migration path named

What's New: Password Manager Desktop Ap… Release Notes 2023 (2026-09-17)

06 **AI Assistant knowledge base uploads** NEW 65

AI Assistant supports knowledge base uploads in PDF, TXT, DOCX, and MD formats, up to 10 MB per file and 25 files per org, with source attribution shown in chat responses.

— Exact formats and size/count limits, no UI path given Release Notes 2026 (2026-09-17)

07 **Bulk credential import into Password Vault** NEW 64

Password Vault supports bulk import of team credentials from a CSV or Excel file exported from a previous password manager, via the User Portal's Password Vault bulk import option.

Bulk-import team credentials into Password Vault from a previous password manager export to eliminate credential sprawl on day one.

📍 1. Log in to the JumpCloud User Portal and open Password Vault from the left navigation. 2. Select the bulk import option and upload a CSV or Excel file containing your credentials.

— Exact file formats and UI path named Release Notes 2026 (2026-09-17)

08 **RSS feeds for release notes and bug fixes** NEW 64

Adds RSS feed subscriptions from the Release Notes and Bug Fixes page: 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.

Subscribe to only JumpCloud product and agent release notes in your RSS reader, filtering out general Help Center noise.

📍 1. Go to the JumpCloud Release Notes and Bug Fixes page. 2. Click Subscribe to Release Notes and Bug Fixes RSS Feed. 3. Open your RSS reader and add the

provided feed URL to begin receiving product release notes and agent release note updates automatically.

— Names all four feed options with a runnable subscription flow

Subscribe to New Feature and Product Up…

THINNER COVERAGE BELOW

09 **Dynamic device groups by attribute rules** IMPROVED 53

Dynamic Device Groups can be created under Device Groups > New Group by enabling Dynamic and adding a rule (e.g. Attribute `Vendor` equals a value) so membership updates automatically as matching devices enroll.

Create a dynamic device group that automatically includes all devices from a specific vendor so new endpoints are governed the moment they enroll.

📍 In the Admin Portal, go to Device Groups › New Group, enable Dynamic, add a rule where Attribute is `Vendor` equals your target value, and save — membership updates automatically as devices enroll.

— Names UI steps and example attribute rule Release Notes 2023 (2026-09-17)

10 **SentinelOne agent deployment via Commands** NEW 51

Adds a SentinelOne integration script usable through the existing Linux Commands feature to silently install the SentinelOne agent across a targeted Linux device group.

Run a SentinelOne agent deployment across all Linux devices in an org using the existing Commands feature.

📍 In the Admin Portal, go to Device Management › Commands, create a new Linux command using the SentinelOne integration script, and target the desired Linux device group to silently install the SentinelOne agent.

— Names integration and command path, no version/limits Release Notes 2022 (2026-09-17)

11 **Default password policy grace-period enforcement** IMPROVED 45

Default password policy enforcement now brings users into compliance on their next password change rather than immediately, with an optional firm compliance date admins can set.

— Describes before/after behavior, no config key named Release Notes 2024 (2026-09-17)

12 **Windows MDM policies via Configuration Service Providers** NEW 43

New Windows MDM policy framework built on Configuration Service Providers (CSPs) lets IT admins configure any company policy directly via CSP.

– Names CSP mechanism but no config example `Release Notes 2024 (2026-09-17)`

13 **Duo Universal Prompt support for MFA** IMPROVED 41

Supports Duo Universal Prompt for MFA ahead of Duo's March 30, 2024 end-of-life for the traditional prompt.

– Names deadline but no config steps `Release Notes 2023 (2026-09-17)`

14 **Manual app tracking in SaaS Management** NEW 38

Admins can manually add apps to SaaS Management to track, warn on, and block them before the app is picked up by automatic discovery.

– Describes capability, no UI path given `Release Notes 2024 (2026-09-17)`

15 **MDM certificate expiration widget** NEW 32

Adds an Upcoming Certificate Expirations widget to the JumpCloud homepage under MDM, giving at-a-glance visibility into certificate lifecycle status.

– Names the widget but no interaction detail `Release Notes 2022 (2026-09-17)`

16 **Interactive password complexity dialog** IMPROVED 27

Adds an interactive, as-you-type password complexity dialog that is mobile-responsive and WCAG-compliant.

– Describes design but not where it appears or config `Release Notes 2022 (2026-09-17)`

17 **Sort Password Manager items by nickname** IMPROVED 23

Password Manager desktop app adds the ability to sort items by nicknames.

– Bare feature name, no UI path given `What's New: Password Manager Desktop Ap…`

18 **Android 15 support in MDM** NEW 21

MDM fully supports Android 15.

– Bare compatibility statement, no detail `Release Notes 2024 (2026-09-17)`

19 **AI Commands Builder** NEW 12

Adds an AI Commands Builder.

– Named only in release summary, no description `Release Notes 2025 (2026-09-17)`

20 **Shadow AI Dashboard** NEW 12

Adds a Shadow AI Dashboard.

– Named only in release summary, no description `Release Notes 2025 (2026-09-17)`

└──▷ **ALSO FROM THESE RELEASES**

Query users whose department contains a pipe character, such as `Finance | Accounting`, alongside other departments in a single API filter call.

```
$ 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'
```

└──▷ **BREAKING ON UPGRADE**

! The JumpCloud Password Manager Linux `.appimage` build is replaced by a Debian (Ubuntu x86) package; existing `.appimage` users must delete their current build and download the new Debian build from the Password Manager downloads page.

! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; replace all usages with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body.

! Dynamic Groups `memberQuery` API filter operators `$le` and `$ge` are deprecated; replace with `$lte` and `$gte` respectively in any API requests using these operators.

! The .appimage Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

---

WAS THIS USEFUL? 👍 👎

# Passbolt

Feedback ⓘ 1 RELEASE · 2026-09-17 NOTES ↗ RANK

Manage and share passwords securely with Passbolt. Open source, audited and built for teams that need collaboration, compliance and control.

> Passbolt introduced a beta Offline Mode that lets users mark resources for offline access and continue signing in, viewing and autofilling selected credentials when the server is unreachable.

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

01 **Offline Mode (Beta) for server outages** NEW 55

Users can mark resources as available offline, then sign in and access those credentials — including read-only access and autofill — when the Passbolt server cannot be reached.



— Describes behaviour and scope but no config key or flag given

Enjoy the Silence | Browser Extension &…

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

## Varonis

Feedback ⓘ 1 RELEASE · 2026-09-15 NOTES ↗ RANK

The leading data and AI security platform that proactively reduces risk, enforces policies, and stops active threats with our AI-native automation.

> Varonis introduced Data Lifecycle Management, a new capability that automatically finds, prioritizes, and quarantines redundant, obsolete, and trivial (ROT) data across connected data sources to cut storage costs and reduce risk.

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

01 **Data Lifecycle Management for ROT data** NEW 60

Data Lifecycle Management (DLM) combines data classification, permissions mapping, and activity analysis to automatically identify, prioritize, and quarantine redundant, obsolete, and trivial (ROT) data — stale, duplicate, overexposed, and expired files — across connected data sources. A ROT dashboard surfaces cost-savings potential and compliance risk areas, lets users drill into any duplicate group to see the original file, where copies live, and which copies are stale, sensitive, or overexposed, and applies configurable, out-of-the-box policies for duplicates, staleness, and retention with fully reversible quarantine.

.
.
.

— Describes mechanism and UI but no config keys or APIs named

Cut storage costs, improve AI outputs, …

WAS THIS USEFUL? 👍 👎

## GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

# RegScale

Feedback ⓘ 1 RELEASE · 2026-09-17 BLOG ↗ RANK

RegScale is a compliance and security governance platform that automates regulatory assessment, documentation, and continuous monitoring across organizations.

> RegScale CLI 6.47.0 adds support for importing JCAM digital identity data covering NIST 800-63 assurance levels and federation rationale.

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

01 **JCAM import for NIST 800-63 digital identity data** NEW

57

The CLI adds JCAM import support for NIST 800-63 digital identity data, including assessed and implemented Identity, Authenticator, and Federation assurance levels, rationale for differences between them, comparability demonstrations, and rationale for not accepting federated identities.

— Names data types and assurance levels but no command or flag CLI 6.47.0 (2026-09-17)

WAS THIS USEFUL? 👍 👎

◆ Compliance Automation & Trust Management

# Compyl

Feedback ⓘ 1 RELEASE · 2026-09-15 NOTES ↗ RANK

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

> Compyl expanded Azure and ServiceNow evidence collection, added AI-powered answer-mapping to Questionnaire Assist, and sped up several syncs by moving them from full rebuilds to incremental updates.

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

01 **AI answer-mapping in Questionnaire Assist** NEW 75

Adds answer-mapping in Questionnaire Assist so AI-generated answers are matched to configured option sets (Yes/No/N/A or maturity scales) with a confidence score and manual review flag for low-confidence results.

— Explains mechanism and behaviour, lacks exact UI path Sep 15th, 2026

02 **Expanded Azure evidence collection coverage** IMPROVED 70

Extends the Azure integration to cover Privileged Identity Management (PIM) role assignments, Entitlement Management access packages, Intune compliance policy status, and backup protected items for automated evidence collection.

— Names four concrete data surfaces, no config detail Sep 15th, 2026

03 **Inline creation on Control and Contract records** NEW 65

Adds inline `+ New` buttons on Control records to create Blueprints and Tasks with automatic linking to the parent Control, and extends this inline creation to Contracts for Vendors, Clients, Assets, and Tasks.

— UI path is clear but no deeper mechanism given Sep 15th, 2026

THINNER COVERAGE BELOW

04 **ServiceNow Service Catalog data ingestion** NEW 57

Extends the ServiceNow integration to ingest Service Catalog Request and Requested Item data, including exception requests, approval workflows, and related records.

— Names data types ingested but no config or endpoint specifics Sep 15th, 2026

05 **Incremental sync for ServiceNow CMDB and Google Workspace Drive**

IMPROVED

55

Switches ServiceNow CMDB syncs from full-table rebuilds to incremental syncs, dramatically reducing sync time for large inventories, and switches Google Workspace Drive file syncs from full rebuilds to incremental syncs, reducing sync time and API usage for large Drive environments.

— Describes mechanism change but no metrics or config keys Sep 15th, 2026

---

06 **Clearer Permission Groups configuration guidance** IMPROVED

30

Adds clearer guidance on the Permission Groups configuration page explaining how it relates to user access.

— Thin documentation-only update with no specifics Sep 15th, 2026

└──▷ **ALSO FROM THESE RELEASES**

---

WAS THIS USEFUL? 👍 👎

◆ Third-Party & Vendor Risk (TPRM)

# Conveyor

Feedback ⓘ 2 RELEASES · 2026-09-09 → 2026-09-15 NOTES ↗

RANK

Conveyor delivers AI for high-stakes customer requests like security reviews, vendor assessments, and requests for proposal (RFP).

> Conveyor's two releases focused on Trust Center access request forms and general app navigation, adding product-line visibility to access approvals and a dockable nav panel, redesigned cmd+k, and a renamed Ask ConveyorAI experience.

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

## 01 Trust Center access request form customization NEW

75

The Trust Center access request form now collects product line interest so approvers can see which product a visitor wants before approving; this is enabled via `Settings > Trust Center > NDA & Access` by turning on Public product lines. The form's description and placeholder text can also be rewritten to collect custom information from visitors upfront.

.
.
.
.

When running multiple products, enable product line selection so access request approvers immediately know which product a visitor needs — no follow-up email required.

> 📍 In the Conveyor console, go to Settings › Trust Center › NDA & Access and enable Public product lines to display them on the Access Request Form.

– Exact settings path and worked example given for both additions

🏷️ Product lines on the Trust Center ac…

THINNER COVERAGE BELOW

## 02 Dockable navigation panel NEW

55

Adds a dockable navigation panel that can be pinned in place via a dock icon to reclaim horizontal screen space, instead of the panel collapsing on mouse-out while working.

Dock the navigation panel to give yourself more horizontal workspace when reviewing questionnaires or trust pages.

📍 In the Conveyor app, click the pin/dock icon on the left navigation panel to lock it in place, then continue working without it collapsing on mouse-out.

— Exact click-path to dock the panel provided 🧭 Easier wayfinding: Dockable nav, a s…

03 **Redesigned cmd+k command palette** IMPROVED 50

`cmd+k` gets a cleaner layout, a products picker matching the launchpad, and an empty-state guide clarifying when you are querying Ask ConveyorAI versus running a keyword search.

— Named UI elements but no runnable steps given 🧭 Easier wayfinding: Dockable nav, a s…

04 **AI Answers renamed to Ask ConveyorAI** IMPROVED 30

The AI Answers feature is renamed to Ask ConveyorAI, with a clearer state displayed when no answer is found.

— Rename and minor behavior change, no usage detail

🧭 Easier wayfinding: Dockable nav, a s…

05 **Consistent headers and breadcrumbs across app** IMPROVED 13

Adds consistent headers and breadcrumbs across the app.

— Bare description with no mechanism or specifics

🧭 Easier wayfinding: Dockable nav, a s…

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

**AGENT**

◆ MCP Servers & Tooling

# Runlayer

Feedback ⓘ 2 RELEASES · 2026-09-16 → 2026-09-17 BLOG ↗

RANK

Runlayer is an MCP gateway that enforces identity-mapped permissions and detects threats across the agents and MCP servers employees use.

> Runlayer's biggest addition this window is DPoP sender-constrained tokens for agent accounts, alongside Enterprise Grok Bot monitoring, calendar-based LLM spend budgets, new ToolGuard threat detection, and new Gmail and Vercel connectors — with two breaking changes to hook behavior.

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

01 **DPoP-bound tokens for agent accounts** NEW 85

Runlayer adds DPoP (RFC 9449) sender-constrained token binding for agent accounts, tying tokens to a client-held ES256 key so a leaked token cannot be replayed. Binding happens at issuance and is enforced at the MCP proxy via a per-agent `require DPoP` flag, toggled in the admin UI under Agents > select agent > Settings.

Enforce DPoP-bound tokens for a specific agent to prevent token replay attacks at the MCP proxy.

> 📍 In the Runlayer admin UI, go to Agents › select the agent › Settings, and enable the `require DPoP` flag. Tokens issued to this agent will be bound to a DPoP key and rejected at the MCP proxy if presented without a valid DPoP proof.

— Names RFC, key type and exact enforcement flag with UI path.

1.28.515 - DPoP-bound agent tokens and …

THINNER COVERAGE BELOW

02 **Calendar-based LLM budget windows** NEW 55

Adds calendar-based budget windows (e.g. monthly caps) to LLM gateway usage rules, letting admins set a period like `monthly` with a token or spend cap per agent.

Cap monthly LLM spend per agent to enforce governance budgets that reset on a calendar cycle.

> 📍 In the Runlayer admin UI, go to Agents › select the agent › Usage Rules, add a budget window, and set the period to `monthly` with your desired token or spend cap.

— Gives UI navigation and concrete monthly-cap example.

1.28.515 - DPoP-bound agent tokens and …

03 **Recursive delete detection in ToolGuard** NEW 55

Adds recursive delete detection to ToolGuard skill scanning, catching combined short-flag recursive deletes such as `rm -rf`.

– Names the exact pattern detected but no trigger or config.

1.28.515 - DPoP-bound agent tokens and …

04 **set_cells in edit_table for Google Docs** NEW 55

Adds `set_cells` capability to the `edit_table` tool for Google Docs, enabling multiple table cells to be set in one call.

– Names exact tool and capability but no usage example.

1.28.515 - DPoP-bound agent tokens and …

05 **Zip skill import** NEW 50

Adds zip skill import, allowing a multi-file skill to be created in one step by importing a single zip file via Skills > Import Skill > Zip import in the admin UI.

Package a multi-file skill and import it in one step rather than uploading files individually.

📍 In the Runlayer admin UI, go to Skills › Import Skill, select Zip import, and upload a zip file containing all skill files. Runlayer will create the multi-file skill from the archive.

– Gives exact UI steps for the import flow. 1.28.515 - DPoP-bound agent tokens and …

06 **Monitor-mode hooks fail open on credential rejection** BREAKING 50

In monitor mode, hooks now fail open (allow) on credential rejection instead of blocking the editor — workflows that previously relied on monitor-mode hooks to block on rejection will no longer be blocked.

– Gives clear before/after behavior for migration awareness.

1.28.478 - Gmail label-added trigger an…

07 **Grok cloud hooks require explicit opt-in** BREAKING 50

Grok cloud hooks now require explicit opt-in and will no longer activate automatically — existing setups relying on automatic Grok cloud hook enrollment will stop working until opted in.

– States the behavior change but not the opt-in mechanism.

1.28.478 - Gmail label-added trigger an…

08 **Per-tool enrollment diff for security settings** NEW

45

Adds a per-tool enrollment diff for recommended security-setting enrollment, showing the effective per-tool diff with scan-direction safety checks before applying.

— Explains what it shows but not where to trigger it.

1.28.515 - DPoP-bound agent tokens and …

09 **Audit events for Slack provisioning and agent runs** IMPROVED

45

Extends audit events to cover Managed Slack provisioning and to carry agent and run IDs on agent-run tool-call events.

— Names the event fields added but no retrieval path.

1.28.515 - DPoP-bound agent tokens and …

10 **View workspace as permission group** NEW

45

Adds a View as permission group capability for Super Admins to view the workspace as any permission group.

— Clear capability but no exact UI path given. 1.28.515 - DPoP-bound agent tokens and …

11 **Gmail label-added poll trigger** NEW

45

Adds a Gmail label-added poll trigger that fires an agent whenever a label is added to a Gmail message.

— Names the trigger and its condition, no setup steps.

1.28.478 - Gmail label-added trigger an…

12 **Central Grok Bot monitoring for Enterprise Teams** NEW

40

Adds Central Grok Bot setup for Enterprise Team deployments, enabling credential provisioning and per-member shadow AI monitoring coverage.

— Describes purpose but no setup steps or config given. product docs

13 **Agent runs continue after approval decisions** IMPROVED

40

Agent runs triggered via MCP or REST now continue after an approval decision, and users can continue their own run from any surface.

— Describes behavior change without a concrete surface or command.

1.28.515 - DPoP-bound agent tokens and …

14 **Default Slack posting identity for agents** IMPROVED

40

Agents now post to Slack as the agent bot by default unless explicitly configured to act as the connected user.

— Explains the new default and the opt-out condition.

1.28.478 - Gmail label-added trigger an…

15 **Vercel OAuth connector** NEW 35

Adds Vercel as a connector available through the OAuth broker.

— Names the connector but no configuration detail.

1.28.478 - Gmail label-added trigger an…

16 **Explanations on rejected access requests** IMPROVED 30

Rejected access requests now include an explanation of why the request was rejected.

— States the change with no detail on where it appears.

1.28.515 - DPoP-bound agent tokens and …

└──▷ **BREAKING ON UPGRADE**

! Grok cloud hooks now require explicit opt-in and will no longer activate automatically — existing setups relying on automatic Grok cloud hook enrollment will stop working until opted in.

! In monitor mode, hooks now fail open (allow) on credential rejection instead of blocking the editor — workflows that previously relied on monitor-mode hooks to block on rejection will no longer be blocked.

WAS THIS USEFUL? 👍 👎

## GOVERN

◆ AI/LLM Security

# Zenity

Feedback ⓘ 1 RELEASE · SEEN 2026-09-17 NOTES ↗ RANK

Zenity discovers, secures and governs enterprise AI agents from buildtime to runtime across SaaS, endpoint and cloud.

> Zenity shipped its first Guardian Agent, Blue Agent, to auto-triage findings, alongside a new Boundaries CLI for policy-as-code, OTel/gen_ai span ingestion for any custom agentic app via the Evaluate API, and GA coverage for GitHub Copilot, OpenAI Codex, and Microsoft Foundry.

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

## 01 Custom Agents integration for OTel and gen_ai spans NEW

95

A new Custom Agents integration ingests OpenTelemetry ( OTel ) and gen_ai spans for visibility and inline enforcement via the Evaluate API , connecting any agentic application to Zenity without a dedicated connector. In the portal, teams go to Integrations > Custom Agents, select the OTel or gen_ai span format, and point their collector at the Evaluate API to verify activity before full onboarding.

Connect a homegrown agentic application to Zenity for visibility and inline enforcement the same day, without waiting for a dedicated integration — any app already emitting OTel spans qualifies.

> 📍 In the Zenity portal, go to Integrations › Custom Agents and select your span format (OTel or gen_ai). Follow the step-by-step guide to point your collector at the Evaluate API endpoint, then verify agent activity appears in the portal before committing to full onboarding.

— Names endpoint, formats, and gives a runnable onboarding path

From Triage to Full Coverage: The Shift…

## 02 Boundaries CLI for policy-as-code NEW

75

A new CLI lets teams manage boundaries, custom taints, and reusable values as version-controlled files, with coding agents like Claude Code and Codex able to author policy directly against Zenity's schema.

— Names CLI and schema but no exact commands shown

From Triage to Full Coverage: The Shift…

## 03 System taints classify tool calls by action type NEW

70

System taints classify tool calls as `read` or mutative operations (`write`, `update`, `delete`, `execute`), enabling Boundaries rules based on what an action does rather than matching command strings or tool names.

– Names taint values and rationale, no exact rule syntax given

From Triage to Full Coverage: The Shift…

04 **Full coverage for Microsoft Foundry** NEW 70

Zenity adds full coverage for Microsoft Foundry (the rebuilt agent stack that replaced Azure AI Foundry at Ignite 2025), including inventory, graph, runtime activity, and AI detection and response (`AIDR`) findings.

– Details scope and context but no setup steps given

From Triage to Full Coverage: The Shift…

05 **Blue Agent triages findings automatically** NEW 65

Blue Agent, the first Guardian Agent, triages every new finding in suggest mode, returning a verdict (benign true positive, false positive, or true positive) with reasoning, confidence level, and full trace attached.

– Explains verdicts and mechanism but no user action described

From Triage to Full Coverage: The Shift…

06 **GitHub Copilot and OpenAI Codex reach GA** NEW 65

GitHub Copilot and OpenAI Codex reach general availability with inventory, activity monitoring, and inline prevention served through hooks.

– Names hooks mechanism but no config detail for setup

From Triage to Full Coverage: The Shift…

07 **Audit log streaming and integration guides for Splunk, Sentinel, Cribl, LiteLLM, Kong**

NEW 65

Zenity added near-real-time audit log event streaming to Splunk or Microsoft Sentinel, and published step-by-step integration guides for Cribl, `LiteLLM`, and Kong to connect agent activity to the Zenity portal.

– Names five platforms and guides though no exact steps included

From Triage to Full Coverage: The Shift…

08 **Boundaries AI assistant drafting and testing** IMPROVED 60

The Boundaries AI assistant can now create required custom taints while drafting a rule, and run draft rules against recent production activity on command before applying them.

– Describes a testable workflow though no exact command shown

From Triage to Full Coverage: The Shift…

THINNER COVERAGE BELOW

09 **Runtime risk signals in Microsoft Agent 365** NEW 45

Zenity runtime risk signals now surface directly inside Microsoft Agent 365, alongside Entra, Purview, and Defender.

— Names surfaces but no mechanism or setup detail

From Triage to Full Coverage: The Shift…

10 **Prevent and Detect labels on taints** IMPROVED 40

Every taint in the Boundaries manager now carries a Prevent or Detect label, showing at a glance whether a rule blocks in real time or flags after the fact.

— Thin one-line UI addition with no further mechanism

From Triage to Full Coverage: The Shift…

WAS THIS USEFUL? 👍 👎

# AI-Infra-Guard

Feedback ⓘ 1 RELEASE · 2026-09-17 NOTES ↗

RANK

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

> AI-Infra-Guard's v4.6.2 release adds two new red-teaming benchmarks for autonomous agents — FORGE-Bench and RogueHandoff-20 — alongside a routine update to its AIG rules dataset.

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

01 **FORGE-Bench loss-of-control benchmark** NEW 60

Adds `forge_bench` (FORGE-Bench), a deterministic Loss-of-Control benchmark for evaluating autonomous agents, including a built-in OpenAI-compatible client and a bilingual quickstart guide.

— Names benchmark and client but no exact commands v4.6.2

THINNER COVERAGE BELOW

02 **RogueHandoff-20 handoff security benchmark** NEW 40

Adds the RogueHandoff-20 benchmark under the Research module for evaluating autonomous agent handoff security.

— Names benchmark and module, no usage detail v4.6.2

03 **AIG rules dataset update** IMPROVED 20

Updates the AIG rules dataset to the 2026-09-11 ruleset.

— Only a date is given, no scope of changes v4.6.2

WAS THIS USEFUL? 👍 👎

## NoLabs nono

Feedback ⓘ 1 RELEASE · 2026-09-16 NOTES ↗ CODE ↗

RANK

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

> nono v0.78.0 adds cryptographically signed, poll-based approval webhooks and a macOS opt-out for implicit DNS grants, while also shipping a prebuilt Nix flake output and stripping out all remaining deprecated CLI surfaces ahead of v1.0.0.

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

01 **macOS DNS opt-out for network modes** NEW 80

Adds CapabilitySet::block_dns() (and the C-API nono_capability_set_block_dns() / nono_capability_set_dns_enabled()) on macOS to let a profile opt out of the implicit `mDNSResponder` grants nono previously added when running in `Blocked` and `ProxyOnly` network modes.

— Names exact API and C-API functions and affected modes. v0.78.0

02 **Prebuilt Nix flake output** NEW 80

Adds a `#prebuilt` Nix flake output that fetches the official release binary directly from GitHub Releases, skipping source compilation — usable via `nix run github:nolabs-ai/nono#prebuilt`.

Install nono instantly in a Nix environment without compiling from source — useful in CI or on machines without a Rust toolchain.

```
$ nix run github:nolabs-ai/nono#prebuilt
```

— Includes a runnable install command. v0.78.0

THINNER COVERAGE BELOW

03 **Removal of deprecated surfaces ahead of v1.0.0** BREAKING 45

All remaining deprecated CLI surfaces and legacy profile aliases have been removed as part of v1.0.0 preparation; any profile or script relying on them will break on upgrade.

— States impact but no specific removed names listed. v0.78.0

└──▷ BREAKING ON UPGRADE

! All remaining deprecated CLI surfaces and legacy profile aliases removed — any profile or script relying on them will break on upgrade.

---

WAS THIS USEFUL?  

# Mend.io Mend AI

Feedback ⓘ 1 RELEASE · 2026-09-16 NOTES ↗

RANK

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> This window's most consequential change is a new install-time authentication requirement for the Guardrails SDK, while Renovate (also shipped under this changelog) gained a release-age buffer config, Dockerfile `apk add` extraction, expanded Forgejo support, a new template helper, and smarter GitHub merge-queue handling.

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

01 **Guardrails SDK install now requires Activation Key** BREAKING

70

The Guardrails SDK installation procedure now requires a Mend Activation Key at download time, in addition to the existing runtime authentication. Existing installations with unpinned versions that attempt to re-install dependencies will now require this Activation Key during the install step.

— Explains before/after clearly but omits the exact install command (16-September-2026)

02 **Forgejo support expanded across Renovate** NEW

68

Adds Forgejo preset references (e.g. `forgejo>`) in `manager/renovate-config`, detects the `forgejo-tags` datasource for git-tag sources in `manager/terragrunt`, and treats Forgejo like Gitea for onboarding-branch rebase and config-hash detection in `workers/onboarding`.

— Names three modules and config surfaces but no full example product docs

THINNER COVERAGE BELOW

03 **minimumReleaseAgeBuffer config option** NEW

56

Adds `minimumReleaseAgeBuffer` config option to control a buffer window around minimum release age checks.

— Named config key but no default value or usage example product docs

04 **Dockerfile apk add dependency extraction** NEW

53

Extracts `apk add` packages from `RUN` instructions in Dockerfiles via `manager/dockerfile`, letting Renovate detect and update these dependencies.

— Names the manager but no config key or example shown product docs

05 **uppercase template helper** NEW 42

Adds an `uppercase` template helper via `util/template` for use in Renovate template expressions.

— Names the helper and module but not an example expression product docs

06 **GitHub direct merge before merge queue** IMPROVED 32

Attempts a direct merge before falling back to the merge queue on `platform/github`.

— Brief mechanism note with no configuration detail product docs

└──▷ **BREAKING ON UPGRADE**

! Existing Guardrails SDK installations with unpinned versions that attempt to re-install dependencies will now require a Mend Activation Key during the install step.

WAS THIS USEFUL?  

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 17, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue