THE CYBER TOOLCHAIN

NO. 074

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 14, 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 50 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 21 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 now flags unpinned dependencies as Potentially Affected for malware, closing the blind where a floating version range could resolve to a poisoned

vim ? help

package. Cloudflare's Passive DLP shows you where sensitive data actually flows before you write a blocking policy. ALEAPP and iLEAPP take raw and E01 images directly, skipping the extraction step.

PROTECT

Catch malicious packages you can't prove you didn't pull

Endor Labs classifies unpinned dependencies as `Potentially Affected` rather than clean, with policy parameters to tune the noise — the gap where a caret range silently resolves to a compromised release. OSV-Scanner now reads Git dependencies natively as `pkg:git` PURLs, so vendored and source-pinned code stops being invisible to the scan, and Cloudsmith exports vulnerability and malicious-package findings as JSON for downstream tracking.

Endor Labs · OSV-Scanner · Cloudsmith

IDENTIFY

See what sensitive data is moving before you block any of it

Passive Detection profiles matches across Gateway traffic without enforcing, so a DLP rollout starts from measured flows instead of a guess. The usual failure — turning on a policy and breaking a business workflow nobody documented — becomes a report you read first.

Cloudflare

RESPOND

Parse a phone image without staging an extraction first

Both now ingest raw disk images and E01 acquisitions directly (`-t raw` in ALEAPP) and parse F2FS, the filesystem on much modern Android. That removes a mount-and-export step per device and keeps the acquisition as the working artifact, alongside new app coverage including Blink, MEGA, Garmin Connect and Tutanota.

ALEAPP · iLEAPP

APPLICATION SECURITY

◆ SAST / SCA / Code Security

ZeroPath

Feedback ⓘ 1 RELEASE · 2026-09-14 CHANGELOG ↗ RANK

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

> ZeroPath's latest release centers on syncing GitHub and Bitbucket repository permissions into its own 39-permission model, alongside new MCP support for AI coding assistants, Microsoft Teams notifications, continuous scanning, and a set of breaking API and permission changes.

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

01 **Access sync and permission import from GitHub and Bitbucket**

NEW 75

ZeroPath now imports repository permissions from GitHub (five roles, including direct collaborators) and Bitbucket (Cloud workspace groups and Server project groups), mapping provider roles onto ZeroPath's own model of 39 permissions across 10 groups.

— Mechanism and scope given, but no UI or API steps to invoke it

changelog-20260914-ed06a3ad

02 **Microsoft Teams notification channel** NEW 65

Scan notifications and vulnerability alerts can be routed to a Microsoft Teams channel via an Incoming Webhook connector, without an Azure AD app registration; the webhook URL is added under Settings -> Connections -> Notifications, with rules to select which events (scan complete, new vulnerability, SLA breach) reach that channel.

Route scan notifications and vulnerability alerts to a Microsoft Teams channel without an Azure AD app registration.

> 📍 In Microsoft Teams: 1. Open the channel you want to receive alerts -> Manage channel -> Connectors -> Incoming Webhook -> Configure. 2. Copy the generated webhook URL. In ZeroPath: 3. Go to Settings -> Connections -> Notifications. 4. Add a new Microsoft Teams channel and paste the webhook URL. 5. Configure notification rules to select which events (scan complete, new vulnerability, SLA breach) reach that channel.

— Concrete UI navigation and webhook setup steps given changelog-20260914-ed06a3ad

03 **Granular permissions for integrations, repositories and ticketing**

65

BREAKING

Connecting an integration now requires the `Create Integrations` or `Create Installations` permission, adding a repository by URL requires `Create Repositories`, and creating Jira and Linear tickets is now a per-repository permission that organizations using access control must explicitly grant.

— Names exact permissions but not how to grant them `changelog-20260914-ed06a3ad`

└──▷ BREAKING ON UPGRADE

- ! On repository objects, `lastScanError` is replaced by `lastScanFailure`; any API consumer reading `lastScanError` will receive no value.
- ! Eleven measurements on the security posture endpoint now return no value where there is nothing to measure — consumers must treat these fields as optional.
- ! On secret findings, the dismissal explanation generated by ZeroPath is withheld from the API response; only a reviewer's own note is returned.
- ! Connecting an integration now requires the `Create Integrations` or `Create Installations` permission; adding a repository by URL requires `Create Repositories`.
- ! Creating Jira and Linear tickets is now a per-repository permission; organizations using access control must explicitly grant it.

WAS THIS USEFUL? 👍 👎

Veracode

Feedback

1 RELEASE · 2026-09-14

CHANGELOG ↗

RANK

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

> Veracode added automated SCA remediation via a new fix command and ended support for its legacy eLearning REST API.

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

01 Automated SCA vulnerability remediation patches NEW

73

After a software composition analysis scan, Veracode can automatically generate a remediation patch for a vulnerable dependency identified in your project, triggered via `veracode fix sca`.

After an SCA scan, automatically generate a remediation patch for a vulnerable dependency identified in your project.

```
$ veracode fix sca
```

— Names the exact command but not scope of supported ecosystems

changelog-20260914-4d08813d

└──▷ **BREAKING ON UPGRADE**

! Veracode eLearning REST API has reached end of support — Veracode will no longer update this API or provide technical support.

WAS THIS USEFUL? 👍 👎

Semgrep

Feedback ⓘ 1 RELEASE · 2026-09-14 CHANGELOG ↗ RANK

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

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

01 **General availability of Autofix** NEW 50

Autofix is now generally available for all customers, running on demand per finding via the finding page or via the API.

— Names entry points but no API endpoint or flag. changelog-20260914-8778169c

└──▷ **BREAKING ON UPGRADE**

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

WAS THIS USEFUL? 👍 👎

Cloudsmith

Feedback ⓘ 2 RELEASES · 2026-09-14 BLOG ↗ RANK

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

> Cloudsmith added two web app features this window: JSON export of vulnerability and malicious package findings, and per-package audit logs.

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

01 Export vulnerability findings as JSON NEW

55

Cloudsmith now lets you export vulnerability and malicious package findings as a JSON file directly from the Cloudsmith web app, useful for offline analysis or compliance reporting. In the web app, navigate to your repository's vulnerability findings view and select the option to export findings as a JSON file, or use the Download vulnerability data option on a package's Overview tab.

Download a snapshot of all vulnerability and malicious package findings for offline analysis or compliance reporting.

> 📍 In the Cloudsmith web app, navigate to your repository's vulnerability findings view and select the option to export findings as a JSON file.

– Names format and UI path but no endpoint or size limits

Download package vulnerability findings…

02 Per-package audit logs NEW

33

Cloudsmith adds a per-package audit trail in the web app showing what changed, who changed it, and when.

– Describes purpose but no fields, retention or access details

Track every change to your packages wit…

WAS THIS USEFUL? 👍 👎

OWASP dependency-track

Feedback ⓘ 1 RELEASE · 2026-09-14

NOTES ↗ RANK

Dependency-Track is a software composition analysis platform that identifies and monitors vulnerabilities in application dependencies and third-party components.

> Dependency-Track 4.14.4 adds support for ingesting and processing SBOMs in the CycloneDX 1.7 schema.

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

01 **CycloneDX 1.7 SBOM support** NEW 40

Dependency-Track can now ingest and process SBOMs using the new CycloneDX 1.7 schema version.

— Names the schema version but no mechanism or scope details. 4.14.4

WAS THIS USEFUL? 👍 👎

Codacy

Feedback ⓘ 1 RELEASE · 2026-09-14 BLOG ↗ RANK

Documentation homepage for the Codacy automated code review tool.

> Codacy introduced Codacy Skills, splitting the offering into a local Analysis CLI Skill for pre-commit scanning and a cloud-backed Code Review Skill for pull request review, both distributed as Claude Code plugins under the Agent Skills standard.

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

01 Analysis CLI Skill for local pre-commit scanning NEW

85

Installable via `npm i -g @codacy/analysis-cli` and `claude plugin install codacy-skills@codacy` (with `claude plugin marketplace add codacy/codacy-skills` to add the marketplace), this skill lets AI agents — Claude Code, OpenAI Codex, GitHub Copilot — run Codacy static analysis locally before a commit, with no Codacy account required. Analysis can be scoped to specific files, staged changes, a branch, or an open pull request via `@codacy/analysis-cli`, and when connected to a Codacy account it syncs local rulesets so checks match the standards enforced at the merge gate. It follows the Agent Skills standard, so it works across multiple coding agents, not just Claude Code.

Install the Analysis CLI and Codacy Skills plugin into Claude Code to enable pre-commit scanning with no account needed.

```
$ npm i -g @codacy/analysis-cli
claude plugin marketplace add codacy/codacy-skills
claude plugin install codacy-skills@codacy
```

— Names install commands, scoping options and ruleset sync mechanism

launch-20260914-e9ff6a7c

02 Code Review Skill for cloud PR reviews NEW

65

Installed via `npm install -g @codacy/codacy-cloud-cli` and authenticated with `codacy login`, the Code Review Skill reviews an open pull request against quality gates, coverage, and cloud analysis results.

Install the Cloud CLI and authenticate to enable the Code Review Skill, which reviews an open PR against quality gates, coverage, and cloud analysis.

```
$ npm install -g @codacy/codacy-cloud-cli
codacy login
```

— Exact install/auth commands given but review mechanism only briefly described

launch-20260914-e9ff6a7c

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

ALEAPP

Feedback ⓘ 1 RELEASE · 2026-09-13 NOTES ↗ CODE ↗ RANK

Android Logs Events And Protobuf Parser

> ALEAPP v2026.4.0 adds direct raw/E01 disk image ingestion via a new `-t raw` flag, F2FS filesystem parsing support, and expanded Android app artifact coverage — full Blink camera/doorbell parsing, MEGA cloud storage caches, and newly named support for Kwai, Avast Cleanup, and YouCam Perfect.

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

01 **Raw/E01 image input via -t raw flag** NEW 85

Adds the `-t raw` flag to read raw disk images and E01 acquisitions directly, enabling forensic analysis without prior extraction. Example usage: `python aleapp.py -t raw -i <path_to_image.E01> -o <path_for_report_output>`.

Parse a raw disk image or E01 acquisition directly without extracting it first — useful when working with full-device forensic captures.

```
$ python aleapp.py -t raw -i <path_to_image.E01> -o
<path_for_report_output>
```

— Names exact flag and includes a runnable command. v2026.4.0

02 **Blink camera/doorbell artifact parsing** NEW 65

Adds full Blink camera/doorbell artifact support for Android, covering Camera Information, Camera Entitlements, Syncmodule Information, Syncmodule Entitlements, and Network Information, all parsed from the BlinkRoom database.

— Lists five specific artifact categories and the source database. v2026.4.0

THINNER COVERAGE BELOW

03 **F2FS filesystem support** NEW 40

Adds F2FS filesystem support via re-vendored `qnxprobe`, allowing ALEAPP to parse Android devices formatted with F2FS.

— Names the underlying library but gives no usage command. v2026.4.0

04 **MEGA cloud storage artifact support** NEW 30

Adds MEGA cloud storage node cache and media caches support for Android.

— Brief description with no further mechanism given. v2026.4.0

05 **New app coverage: Kwai, Avast Cleanup, YouCam Perfect** NEW

15

Adds new Android app coverage for Kwai, Avast Cleanup, and YouCam Perfect, named in the release summary but without artifact-level detail in this window.

— Only named in summary; no artifact or mechanism detail provided. v2026.4.0

WAS THIS USEFUL? 👍 👎

iLEAPP

Feedback ⓘ 1 RELEASE · 2026-09-13 NOTES ↗ CODE ↗ RANK

iOS Logs, Events, And Plist Parser

> iLEAPP v2026.4.0 adds direct CLI parsing of raw disk images and E01 acquisitions with new F2FS filesystem support, plus new artifact coverage for Garmin Connect, Tutanota, MEGA, and expanded SMS/WhatsApp/WiFi/KML reporting.

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

01 **Raw disk image and E01 input type** NEW 75

Adds `-t raw` input type to parse raw disk images and E01 acquisitions directly from the CLI.

— Names exact CLI flag and supported formats v2026.4.0

02 **SMS preview attachment and metadata reporting** NEW 70

Adds the `apple_sms_preview_ktx_atx` artifact (SMS & iMessage category) to surface Apple SMS preview attachments stored as ATX containers with `.ktx` extensions under `com.apple.MobileSMS/Previews/Attachments/`, and adds a Shared Name column to the Apple SMS Preview Cache artifact reporting contact card and location share titles from companion plists.

— Names artifact key, path, extension and new column v2026.4.0

03 **F2FS filesystem support for raw images** NEW 65

Adds F2FS filesystem support via re-vendored qnxprobe 1.28/1.29, enabling raw image parsing of F2FS volumes.

— Names library versions but not invocation v2026.4.0

THINNER COVERAGE BELOW

04 **New artifacts for Garmin Connect, Tutanota, and MEGA** NEW 45

Adds full artifact coverage for Garmin Connect on iOS, including the Move IQ activity series, plus new artifact coverage for Tutanota and for MEGA cloud storage.

— Names apps but no schema or fields given v2026.4.0

05 **WiFi geotag linking in Known Networks artifact** IMPROVED 30

Links WiFi network store geotags to their networks through recorded relationships in the WiFi Known Networks artifact.

— Names artifact but not the relationship mechanism v2026.4.0

06 **Timestamp-based KML placemark naming** IMPROVED 30

Names KML placemarks by timestamp in two location artifacts for clearer geographic reporting.

— Two artifacts affected but not identified v2026.4.0

07 **Expanded WhatsApp call record parsing** IMPROVED 20

Expands WhatsApp call record parsing to include additional call record fields on iOS.

— No fields named, vague scope v2026.4.0

WAS THIS USEFUL? 👍 👎

Mobile Verification Toolkit

Feedback ⓘ

1 RELEASE · 2026-09-14 | NOTES ↗ | CODE ↗ | RANK

MVT (Mobile Verification Toolkit) helps with conducting forensics of mobile devices in order to find signs of a potential compromise.

> MVT's latest release focuses on forensic accuracy and robustness: bugreport analysis now respects device timezones, IOC loading is deferred for efficiency, and corrupted sysdiagnose archives fail gracefully instead of silently aborting.

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

01 **Timezone-aware bugreport timestamp analysis** NEW 86

Adds `--timezone` / `-t` option to `mvt-android check-bugreport`, accepting an IANA timezone name (e.g. `Europe/Paris`), so bugreport file timestamps are interpreted in the device's wall-clock zone rather than the analysing machine's timezone. If not specified, it falls back to reading `persist.sys.timezone` from the bugreport's `SYSTEM PROPERTIES` section automatically.

Analyse a bugreport from a device known to be in a specific timezone when `persist.sys.timezone` is absent or unreliable in the archive.

```
$ mvt-android check-bugreport --timezone 'America/New_York' -o
./results/ bugreport-2026-09-14.zip
```

— Full mechanism, fallback behaviour, and runnable command given. v2026.9.14

02 **Graceful handling of corrupted sysdiagnose archives** IMPROVED 62

Unreadable or truncated sysdiagnose archives now trigger a critical-level log message and a clean exit code 1, instead of a silent 'Aborted!'. This is achieved by catching `tarfile.ReadError`, `EOFError`, `zlib.error`, and `OSError`.

— Names exact exceptions and exit behaviour, but no user command. v2026.9.14

THINNER COVERAGE BELOW

03 **Deferred STIX IOC loading** IMPROVED 48

`mvt-android` and `mvt-ios` subcommands that list modules or reject invalid paths no longer parse IOC files unnecessarily, since STIX indicator loading is now deferred until first use.

— Explains behaviour change but no direct user action. v2026.9.14

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Clavister Knowledge Base

Feedback ⓘ

1 RELEASE · 2026-09-14 BLOG ↗ RANK

Clavister Knowledge Base is a technical documentation repository providing security solutions, product information, and support resources.

> Clavister NetWall gained the ability to act as a DNS-over-TLS (DoT) gateway.

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

01 **DNS-over-TLS gateway support in NetWall** NEW 45

NetWall can now terminate DNS-over-TLS (DoT) connections by configuring the cOS Core TLS functionality within an IP Policy.

— Names cOS Core TLS and IP Policy but no config steps

Using NetWall as a DNS-over-TLS (DoT) G…

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Trend Vision One

Feedback ⓘ 2 RELEASES · 2026-09-14 BLOG ↗

RANK

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

> Trend Vision One shipped faster device posture reporting for its Windows Zero Trust Secure Access module and expanded ChatGPT traffic inspection with an updated Prompt Scan engine on the On-Premises Gateway.

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

01 **Faster device posture reporting interval** IMPROVED 40

The Zero Trust Secure Access Module for Windows reduces the device posture reporting interval from 5 minutes to 2 minutes, enabling faster detection of posture changes.

— Clear before/after numbers but no config surface

Zero Trust Secure Access Module for Win…

02 **ChatGPT unauthenticated traffic inspection and Prompt Scan update**

NEW 40

The Zero Trust Secure Access On-Premises Gateway adds support for ChatGPT unauthenticated traffic inspection, covering sessions where users have not signed into ChatGPT, and adopts the latest Prompt Scan engine to improve detection accuracy for prompt injection and harmful prompts.

— Names the capability and engine but no config detail

Zero Trust Secure Access On-Premises Ga…

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

OpenCTI

Feedback ⓘ 1 RELEASE · 2026-09-14 NOTES ↗ RANK

Open Cyber Threat Intelligence Platform

> OpenCTI added support for custom map tile sources and improved reliability for deployments behind load balancers.

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

01 **Custom PMTiles map source** NEW 60

Admins can upload a custom PMTiles file as the map source; it is stored in S3-compatible storage (Silo or any S3-compatible storage) and replaces the previous file on upload, becoming active immediately with no extra steps.

— Names storage mechanism and upload behavior but no exact config path. product docs

THINNER COVERAGE BELOW

02 **Configurable keep-alive and headers timeout** IMPROVED 45

Adds configurable keep-alive and headers timeout settings for deployments behind a load balancer (ALB/ECS), addressing intermittent 502 errors.

— Describes purpose and target setup but no exact setting names. 7.260914.0

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Intruder

Feedback ⓘ changelog · Sep 14, 2026 CHANGELOG ↗

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

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

└──▷ HOW TO FIND IT

Include an API subdomain and an external identity provider in an authenticated scan so the crawler can follow full application flows without hitting domain boundaries.

> 📍 In the Intruder console, open your web app target and go to Authentication settings. Locate the Additional domains field and add entries such as `api.example.com` and `auth.example.com`, then save and re-run the scan.

Adds an Additional domains field when setting up or editing authentication for a web app target, allowing trusted subdomains (e.g. `api.example.com`, `auth.example.com`) and external services (identity providers, CDNs, third-party APIs) to be included in authenticated scan scope.

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

OSV-Scanner

Feedback ⓘ 1 RELEASE · 2026-09-14 NOTES ↗ RANK

Vulnerability scanner written in Go which uses the data provided by https://osv.dev

> OSV-Scanner v2.6.0 adds an experimental-plugins flag for extra file-type extractors, native Git dependency detection via pkg:git PURLs, and a multi-arch container image, alongside smaller improvements to SPDX output and gRPC retry handling.

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

01 **Experimental extractor plugins flag** NEW 77

The `--experimental-plugins` flag enables additional file-type extractors that are not on by default; supported extractor names are documented in the Supported Inventory Types doc. Example: `osv-scanner scan source --experimental-plugins -r /path/to/your/dir`.

Scan a directory using experimental extractors to cover newly supported file types not yet enabled by default.

```
$ osv-scanner scan source --experimental-plugins -r
/path/to/your/dir
```

— Runnable command given but new extractor names not listed v2.6.0

02 **Git-pinned dependency detection with pkg:git PURLs** NEW 60

OSV-Scanner now extracts Git repository URLs and supports local OSV tag matching for Git-based dependencies, typing them as `pkg:git` PURLs. This applies to JavaScript lockfiles including `package-lock.json`, `yarn.lock`, `pnpm-lock.yaml`, and `bun.lock`.

— Names lockfiles and PURL type but gives no command v2.6.0

THINNER COVERAGE BELOW

03 **SPDX output retains unversioned packages** IMPROVED 40

SPDX output now retains packages that lack a version or PURL, and merges related packages based on lineage relationships.

— Describes behaviour change but no example or flag v2.6.0

04 **Multi-arch container image for scanner action** NEW

30

Publishes a multi-arch (`linux/arm64`) container image for `osv-scanner-action` .

— Bare fact with no usage detail v2.6.0

05 **gRPC retry backoff for scalibr plugins** IMPROVED 30

Configures a retry policy with exponential backoff for transient gRPC errors in scalibr plugins.

— Mechanism named but no config surface or example v2.6.0

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Didit

Feedback ⓘ 1 RELEASE · 2026-09-14 CHANGELOG ↗ RANK

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

> Didit's latest release enriches session results for digital-ID-wallet verifications with credential detail, adds a billing-rate preview to console lookup switches, and exposes per-country configuration for non-document ID lookup with retry and fallback controls.

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

01 Per-country non-document lookup configuration NEW

92

Non-document lookup can be enabled per country in the ID Verification step, letting users verify with just their national ID number instead of uploading a document. In the Didit console, open your workflow, select the ID Verification step, go to the Countries tab, choose the target country, and toggle the non-document lookup method on; set the retry count (1–5) and choose a fallback action for each failure mode (partial match, no match, no source response).

Enable non-document lookup for a specific country so users can verify with just their national ID number instead of uploading a document — useful for markets where lookup sources have high coverage.

📍 In the Didit console, open your workflow, select the ID Verification step, go to the Countries tab, choose the target country, and toggle the non-document lookup method on. Set the retry count (1–5) and choose a fallback action for each failure mode (partial match, no match, no source response).

— Exact console navigation, tab name, and retry/fallback parameters given.

changelog-20260914-1233caae

THINNER COVERAGE BELOW

02 Credential details in wallet verification results NEW

42

Session results for digital-ID-wallet verifications now include credential details: the wallet used, its issuing authority, the level of assurance asserted, and whether the signature checked out.

— Names the data fields added but no API path or schema. changelog-20260914-1233caae

03 **Cost preview for console lookup switches** NEW 33

The Didit console now shows a cost preview when configuring lookup switches: each lookup switch displays its billing rate before the configuration is saved.

— Describes UI behaviour but no exact navigation path. changelog-20260914-1233caae

WAS THIS USEFUL? 👍 👎

ConductorOne

Feedback ⓘ 1 RELEASE · 2026-09-14 CHANGELOG ↗

RANK

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

> ConductorOne replaced its single Product digest view with per-section overview dashboards across the admin nav, added a configurable bulk-request cap, and shipped role mining, access graph, and anomaly-detection UI improvements — alongside two breaking changes to automation expression syntax and the Findings Owner field.

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

01 Anomaly detection pause for membership automation NEW

60

The membership automation edit drawer adds an Anomaly detection section with a Pause automation when anomalies are detected toggle and a view of removed members, allowing automations to halt when unusual membership changes occur.

— Names toggle and section but not exact configuration path changelog-20260914-87306871

THINNER COVERAGE BELOW

02 Per-section overview dashboards across admin nav NEW

45

Adds dedicated overview dashboards to each major admin nav section, such as Identities & NHI (with tabs and stat tiles for human users, service accounts, secrets, agents, and NHI counts), replacing the single Product digest view that previously aggregated this information.

— Names replaced view and one dashboard but no exact nav path changelog-20260914-87306871

03 Access graph highlights matched entitlement grants NEW

30

The access graph for a requested entitlement now shows its granted repositories with the searched-for repository highlighted as a match.

— Thin description with no navigation or scope details changelog-20260914-87306871

└──▷ **BREAKING ON UPGRADE**

! Automation expressions that reference the bare workflow context, or pass it directly to a function, no longer compile — expressions must name the step and field directly. Any

automation using an indirect-reference expression will fail to save on next edit until rewritten to a static path.

! The `Owner` column, filter, detail field, API field, and audit-log event names on Findings are renamed to `Assignee` — integrations consuming the Finding object via API, webhook, or SIEM audit log must update to the new field and event names.

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ 1 RELEASE · 2026-09-14 CHANGELOG ↗ RANK

JumpCloud makes it simple to manage Windows, Apple, Linux, and Android devices and to deliver secure access with SSO, MFA, Zero Trust, RADIUS, and more.

> JumpCloud expanded its AI Gateway with MCP server connection status tracking, a guided Add MCP Server workflow, and mandatory app-based access scoping (with related breaking changes), while also adding AI agent identity registration, device-level MCP discovery with token/cost tracking, and a Custom Query Builder for compliance reporting.

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

01 AI agent identity registration with OAuth credentials NEW

70

Admins can register an AI agent identity under Identity Management > Agents, filling in name, owner, and company email, then generating OAuth client credentials on the Authentication tab so the agent can authenticate to JumpCloud resources, including the AI Gateway, independently of a human account.

Register an AI agent identity and configure OAuth credentials so an AI agent can authenticate to JumpCloud resources independently of any human account.

> 📍 In the Admin Portal, go to Identity Management › Agents and click + Add. Fill in the agent name, owner, and company email on the Details tab, then open the Authentication tab and generate OAuth client credentials for the JumpCloud AI Gateway.

— Exact navigation and steps make it directly actionable. changelog-20260914-6fcef65f

02 MCP connection status and Add MCP Server workflow NEW

65

The AI & SaaS Management Applications tab now shows an MCP Connection Status column with values `Discovered`, `Connected`, and `Not Available`, and a new `Add MCP Server` workflow lets admins connect discovered MCP servers to AI Gateway without leaving the applications view.

.
.
.
.

— Names UI location and status values but not a runnable command.

changelog-20260914-6fcef65f

└──▷ **BREAKING ON UPGRADE**

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

! The custom app creation option has been removed from the Add MCP Server dialog; admins must use `+ New App` to open the standard Add New SSO Application wizard when creating an app during server setup.

WAS THIS USEFUL? 👍 👎

1Password

Feedback ⓘ 1 RELEASE · 2026-09-14 CHANGELOG ↗ RANK

All the latest releases from the 1Password team

> 1Password's browser extension now fully supports passkeys, and Watchtower can identify existing logins that are eligible to be upgraded to one.

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

01 Passkey support with Watchtower upgrade alerts NEW

60

The 1Password browser extension now ships full passkey support, letting users create and save passkeys for sites directly from the extension. Watchtower has been updated to flag logins that can be upgraded to a passkey, so users can find and switch eligible accounts without manually checking each site.

Find which of your saved logins can be hardened by switching to a passkey, without manually checking each site.

> 📍 In 1Password, open Watchtower. Review the new passkey upgrade alerts — each flagged login identifies an account where you can replace your password with a passkey. Select a login and follow the prompt to create and save the passkey for that site.

— Names Watchtower and browser extension, gives a clear UI path.

changelog-20260914-a09dc10e

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

Zscaler

Feedback ⓘ 1 RELEASE · 2026-09-14 BLOG ↗ RANK

Zscaler is a cloud-based security platform that inspects and filters internet traffic to protect organizations from cyber threats.

> Zscaler launched Zero Trust Exchange Agentic Operations, a new AI-driven operational layer pairing a hosted MCP server with the native ZAgent assistant, alongside OAuth 2.1-based governance controls for connecting and auditing third-party and custom AI agents.

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

01 Zero Trust Exchange Agentic Operations with ZAgent NEW

70

Introduces Zero Trust Exchange Agentic Operations, a new hosted operational layer exposing intent-based tools and skills to first-party and third-party AI agents via a hosted Model Context Protocol (MCP) server. Includes ZAgent, Zscaler's native agentic experience within the Experience Center, letting administrators describe objectives in natural language and receive coordinated responses from specialized Zscaler agents and skills.

Investigate why a user cannot reach a business-critical application using ZAgent in the Experience Center, without manually navigating multiple consoles or logs.

> 📍 In the Experience Center, open ZAgent and type: 'Why can't [user] reach the finance application?' — ZAgent routes the request to the appropriate Zscaler agents and skills, gathers context, and returns a likely cause and recommended remediation.

— Names MCP server and ZAgent with a worked example, but no config/API detail

2026-09-14-ddbcce12

02 OAuth-based agent authorization and governance NEW

70

Supports connecting approved commercial AI clients (Claude, ChatGPT) and custom customer-built agents through an OAuth 2.1 authorization flow, with per-user role-scoped consent and revocation. An Agentic Operations Gateway handles routing, identity, authorization, approval controls, and auditing for all agent interactions, with client registration and token lifecycle events recorded in Zscaler audit logs. Super Administrators can review and revoke authorization grants across the entire organization from a central view.

— Names OAuth 2.1, clients, and audit logging but no exact command or endpoint

2026-09-14-ddbcce12

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ 1 RELEASE · 2026-09-13 NOTES ↗

RANK

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 200+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

> CISO Assistant v4.0.3 gives admins the ability to enforce a single date format across all users on an instance.

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

01 **Admin-enforced date format setting** NEW 33

Admins can now force a single date format to apply for all users across the instance, standardizing how dates are displayed platform-wide.

— States the change but no config key or UI path given v4.0.3

WAS THIS USEFUL? 👍 👎

◆ Continuous Control Monitoring (CCM)

RegScale

Feedback ⓘ 1 RELEASE · 2026-09-13 BLOG ↗ RANK

RegScale is a compliance management platform that automates regulatory assessments, documentation, and audit workflows for organizations.

> RegScale's CLI added three new integration subcommands for third-party security data ingestion, deprecated the CSAM subcommand in favor of JCAM, and improved JCAM configuration checks with empty-role detection alongside new CLI-based service account management.

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

01 **Empty-role detection in jcam check_config** IMPROVED

80

`regscale jcam check_config` now detects any role declared in `jcamSystemRoles` that matches no point-of-contact position in any JCAM system in scope, surfacing roles that would be created empty before they are built.

Catch unmatched roles in your JCAM configuration before provisioning, so no empty roles are created in scope.

```
$ regscale jcam check_config
```

— Names config key, mechanism, and a runnable command example. CLI 6.46.0 (2026-09-13)

THINNER COVERAGE BELOW

02 **New integration subcommands: archer, ibm, veracode** NEW

55

Adds `archer` subcommand for RSA Archer bidirectional integration, including login and sync commands, `ibm` subcommand for IBM AppScan file processing, and `veracode` subcommand to process Veracode export files.

— Names three subcommands but no flags or file formats detailed. product docs

03 **Service account management from the CLI** NEW 30

Adds ability to create and manage RegScale service accounts from the CLI.

— No commands, flags, or scope detailed. CLI 6.46.0 (2026-09-13)

└──▷ **BREAKING ON UPGRADE**

! The `csam` subcommand is deprecated; DoJ renamed CSAM to JCAM — use `regscale jcam` instead.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 14, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ **Subscribe** Feedback on this issue