THE CYBER TOOLCHAIN

NO. 073

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 13, 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 80 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 16 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. JumpCloud gave AI agents their own identity records and shipped a password vault, so agent access stops on a human's credentials. Veracode's `veracode fix sca` writes

vim ? help

the dependency patch and safe upgrade path from the terminal. RegScale added 60+ CLI integration commands, pulling SIEM, CNAPP and scan-file evidence into compliance work without the console.

PROTECT

Fix a vulnerable dependency from the terminal instead of hand-reading the upgrade matrix

`veracode fix sca` generates patches and safe upgrade paths for vulnerable dependencies at the command line, and Semgrep's Autofix is now on for everyone — the step that disappears is a developer manually working out which minor bump actually clears the CVE without breaking the build. Socket's Coana engine adds PHP/Composer, Rust/Cargo and multi-root JVM reachability, so the triage list shrinks to dependencies whose vulnerable code is actually called.

Veracode · Semgrep · Socket

PROTECT

Give an AI agent its own identity rather than letting it borrow a human's

JumpCloud's Agent Identities create a non-human identity layer for AI agents, with MCP usage discovery to surface where agents are already reaching; ConductorOne adds call-time classifiers on agent actions. Until now agents typically ran on a service account or a developer's token, which means no way to revoke one agent, and no audit trail that distinguishes it from the person it borrowed from.

JumpCloud · ConductorOne

PROTECT

Cover the login surfaces that a single-target scan or a password-only vault misses

Intruder's Additional domains field lets an authenticated web app scan reach the API backend and auth provider on separate subdomains in one run, instead of leaving the parts of the app that actually hold the session untested. 1Password now creates, manages and shares passkeys across extension and native apps, with Watchtower flagging logins ready to move off passwords.

Intruder

◆ Post-Exploitation

evil-winrm-py

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

Execute commands interactively on remote Windows machines using the WinRM protocol (just faster)

> evil-winrm-py v1.7.0 adds an MCP server mode that exposes WinRM sessions as tools for AI agents, plus support for connecting to constrained JEA endpoints.

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

01 **MCP server mode for AI agent access** NEW 90

A new `--mcp` flag starts evil-winrm-py as an MCP server in streamable HTTP mode, configurable with `--mcp-host` (default `127.0.0.1`) and `--mcp-port` (default `8000`). It exposes four MCP tools — `winrm_login`, `winrm_execute`, `winrm_logout`, and `list_sessions` — supporting multiple concurrent WinRM sessions each tracked by a `session_id`.

Expose a WinRM session as MCP tools for an AI agent to authenticate and run commands against a Windows host.

```
$ evil-winrm-py --mcp --mcp-host 127.0.0.1 --mcp-port 8000
```

— Names exact flags, defaults, and all four MCP tools with a runnable example. v1.7.0

02 **JEA endpoint support via -c flag** NEW 85

A new `-c` / `--configuration-name` CLI flag connects to a constrained JEA endpoint instead of the default `Microsoft.PowerShell` full PowerShell session, available in both interactive shell and MCP server modes. Remote tab-completion adapts to the commands available on the connected JEA endpoint, and menu commands unsupported under JEA are automatically disabled in the interactive shell.

Connect to a restricted JEA endpoint on a Windows host to operate within a least-privilege PowerShell session configuration.

```
$ evil-winrm-py -i 192.168.1.100 -u operator -p P@ssw0rd -c
JEA_Endpoint
```

— Names the exact flag, default endpoint, and behavioral adaptations with a runnable example.

v1.7.0

THINNER COVERAGE BELOW

03 **NO_COLOR environment variable support** IMPROVED 40

evil-winrm-py now respects the `NO_COLOR` environment variable to suppress color output.

— Names the exact env var but no further mechanism given. v1.7.0

04 **Optional path arguments for upload/download** IMPROVED 40

The `upload` menu command's `remote_path` and the `download` menu command's `local_path` are now optional arguments.

— Names the exact commands and parameters made optional. v1.7.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

ZeroPath

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

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

> ZeroPath shipped a remote MCP server for AI coding assistants, a Continuous Scanning mode that rescans on every commit, and a new Assistant skills/plan-first system, alongside Microsoft Teams notifications, scanner workspace and permission reorganization, higher validation coverage, broader language support for repo sizing, and several breaking API response changes.

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

01 **Remote MCP server for AI assistants** NEW 85

Adds a remote MCP server at `https://zeropath.com/mcp` supporting Streamable HTTP clients such as Claude, Cursor, and Codex. Connections are read-only until explicitly approved, and administrators can view and revoke all connections organization-wide.

Connect an AI coding assistant to your ZeroPath findings without installing anything or managing API keys.

📍 # In Claude, Cursor, Codex, or any Streamable HTTP MCP client, # set the MCP server URL to: `https://zeropath.com/mcp` # Then authenticate via browser when prompted. The session is read-only until you explicitly approve changes.

— Names exact URL and connection model with a runnable setup example.

changelog-20260913-ed06a3ad

02 **Continuous Scanning mode** NEW 75

Adds Continuous Scanning mode: triggers a full scan on every meaningful commit to a repository's default branch (including merged pull requests), re-examines what changed on follow-up scans, and closes findings fixed by those commits. Available on GitHub, GitLab, Bitbucket Cloud, and Bitbucket Server, and configurable per organization, tag, or repository.

— Detailed mechanism and platform scope, but no direct command shown.

changelog-20260913-ed06a3ad

03 **Breaking changes to API response fields** BREAKING 75

On repository objects, `lastScanError` is replaced by `lastScanFailure`; consumers reading `lastScanError` will receive no value and must switch. Eleven

measurements on the security posture endpoint now return no value where there is nothing to measure, so consumers must treat these fields as optional. On secret findings, the dismissal explanation generated by ZeroPath is withheld from API responses; only a reviewer's own note is returned.

— Names exact fields and behavior changes consumers must handle.

changelog-20260913-ed06a3ad

04 **Microsoft Teams notifications via Adaptive Cards** NEW

65

Adds Microsoft Teams channel notifications rendered as Adaptive Cards; a channel owner pastes an incoming webhook URL into ZeroPath with no Azure AD app registration required, and notification rules control which events reach which channels.

— Clear setup steps but no exact config key or endpoint given.

changelog-20260913-ed06a3ad

05 **Consolidated Scanner workspace** IMPROVED

60

Adds a Scanner workspace consolidating all scan-configuration pages under a single sidebar entry: Configuration (scanner settings and scan locations) and Detection (repository context, rules, sources and sinks).

— Names the consolidated pages but only points to a UI location.

changelog-20260913-ed06a3ad

06 **Scoped scanner permissions** NEW

60

Adds scoped scanner permissions so that rules, repository context, and scan location pages reflect the actions a member holds; the Teams permission editor now lists every grantable permission.

— Names the affected pages but no exact permission keys given.

changelog-20260913-ed06a3ad

THINNER COVERAGE BELOW

07 **Plan-first mode for Assistant** NEW

55

Adds `Plan first` mode for the Assistant: proposes an editable plan before anything runs, with the option to save the approved plan as a schedule, trigger, or playbook.

— Describes the workflow but lacks a concrete command or config.

changelog-20260913-ed06a3ad

08 **Repository size measurement for more languages** NEW

50

Adds `Terraform`, `Svelte`, `Vue`, `Solidity`, `Elixir`, `Dart`, `protobuf`, and `Genero` to repository size measurement, enabling analysis-depth scaling for those codebases.

— Lists all eight languages verbatim but describes no user action.

changelog-20260913-ed06a3ad

09 **Higher final validation coverage** IMPROVED 45

Raises final validation coverage to up to 1,000 findings per scan, up from 50.

— Gives exact before/after numbers but no user-facing action. changelog-20260913-ed06a3ad

10 **PR address in scan webhooks** IMPROVED 30

Adds pull request address to pull request scan webhooks.

— One-line addition with no field name or schema detail given.

changelog-20260913-ed06a3ad

└──▷ **BREAKING ON UPGRADE**

! On repository objects, `lastScanError` is replaced by `lastScanFailure`; any API consumer or integration reading `lastScanError` will receive no value and must update to `lastScanFailure`.

! 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 API responses; only a reviewer's own note is returned.

WAS THIS USEFUL? 👍 👎

Veracode

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

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

> Veracode's biggest addition this cycle is a `veracode fix sca` CLI command that generates patches and safe upgrade paths for vulnerable dependencies directly from the command line, alongside new language support in Static Analysis and a usage analytics dashboard; the legacy eLearning REST API has reached end of support.

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

01 **`veracode fix sca` CLI command** NEW 75

A new CLI command, `veracode fix sca`, remediates vulnerable SCA dependencies identified in a scan by generating patches and safe upgrade paths directly from the CLI.

Remediate vulnerable SCA dependencies identified in a scan by generating patches and safe upgrade paths directly from the CLI.

```
$ veracode fix sca
```

— Runnable command with clear purpose given changelog-20260913-4d08813d

THINNER COVERAGE BELOW

02 **New language and framework support in Static Analysis** NEW 50

Static Analysis now supports Dart 3.13, Flutter 3.47, PHP 8.4, and PHP 8.5.

— Names exact versions but no usage detail changelog-20260913-4d08813d

03 **Improved CWE-80 detection for React useState** IMPROVED 45

Improves detection of CWE-80 (basic XSS) flaws involving React `useState` in Static Analysis.

— Names the CWE and specific React pattern changelog-20260913-4d08813d

04 **GitHub Workflow SCA fix generation** NEW 25

Adds GitHub Workflow SCA fix generation, referenced only in the release summary with no further mechanism described.

— Mentioned only in summary, no detail given changelog-20260913-4d08813d

└──▷ **BREAKING ON UPGRADE**

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

WAS THIS USEFUL?  

Semgrep

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

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

> Semgrep rolled out Autofix to all customers, added webhook notifications for Supply Chain incident policies, and made several smaller improvements to the Issues API, Agentic Workflows triage, and Workflow jobs filtering, while dropping Homebrew support on Intel Macs.

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

01 Webhook actions on Supply Chain incident policies NEW

70

You can now add a webhook action to Supply Chain incident policies, such as the Early notification for Supply Chain incidents policy, so your security team is notified of new incidents in real time. Configure it in the console via Policies > [policy name] > Actions > Add action > Webhook, entering your webhook URL.

Add a webhook action to the Early notification for Supply Chain incidents policy so your security team is notified of new incidents in real time.

> 📍 In the Semgrep console, go to Policies › Early notification for Supply Chain incidents › Actions, click Add action, select Webhook, and enter your webhook URL.

— Exact UI navigation steps make this directly usable changelog-20260913-8778169c

THINNER COVERAGE BELOW

02 Autofix enabled for all customers IMPROVED

55

Autofix is now enabled for all customers; it remains opt-in per finding and runs only when requested from the finding page or through the API.

— Names entry points but no exact API call or limits changelog-20260913-8778169c

03 Supply Chain Autofix decoupled from Upgrade Guidance IMPROVED

55

Supply Chain Autofix is now independent of Upgrade Guidance, allowing Autofix pull requests to be opened even when Upgrade Guidance is disabled or has not yet run.

— Clear before/after but no concrete command or config changelog-20260913-8778169c

04 Homebrew install dropped for Intel Macs BREAKING

45

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

– States the break but no migration path given changelog-20260913-8778169c

05 **Ignore reason and comment for Agentic Workflows triage** NEW

30

You can now record an ignore reason and a comment when triaging an Agentic Workflows issue.

– Describes the action but no UI path or API detail changelog-20260913-8778169c

06 **Persisted Workflow jobs filters** IMPROVED

30

Workflow jobs filters now persist across page refreshes and navigation.

– States the behavior change with no further mechanism changelog-20260913-8778169c

07 **Expanded Issues API fields** IMPROVED

10

The Issues API now exposes additional fields, though the changelog does not specify which fields were added.

– Only a bare mention with no field names given changelog-20260913-8778169c

└──▷ **BREAKING ON UPGRADE**

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

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

Yamato Security Hayabusa

Feedback ⓘ

1 RELEASE · 2026-09-12 NOTES ↗ CODE ↗ RANK

Hayabusa (隼) is a sigma-based threat hunting and fast forensics timeline generator for Windows event logs.

> Hayabusa v4.1.0 adds a sort-csv command for merging and deduplicating scan output, enriches logon-summary with GeoIP and RDP session data, and widens extract-base64 PowerShell coverage.

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

01 sort-csv command for CSV deduplication NEW

90

New `sort-csv` command sorts a Hayabusa CSV by `Timestamp` and deduplicates detections by comparing every column except `EvtxFile`. It accepts a single file via `-f, --file`, a directory of CSVs via `-d, --directory`, an output path via `-o, --output`, and `-C, --clobber` to overwrite existing output.

Merge and deduplicate CSVs collected from multiple endpoints (e.g. via Velociraptor) into a single chronologically sorted output file.

```
$ hayabusa sort-csv -d ./endpoint-csvs/ -o merged-timeline.csv -C
```

— Full command, flags, and dedup mechanism given with a runnable example. v4.1.0

02 GeoIP enrichment and expanded logon-summary aggregation

IMPROVED

90

The `logon-summary` command gains a `-G, --geo-ip` option that appends `Source ASN`, `Source Country`, and `Source City` columns for the source IP of each summarized logon. It also adds `First Logon` / `Last Logon` columns to the successful logon table and `First Attempt` / `Last Attempt` columns to the failed logon table, and now aggregates RDP session events from Security event IDs `4778` / `4779`, Terminal Services RemoteConnectionManager/Operational `1149`, and LocalSessionManager/Operational `25`, in addition to the existing `21` and `302` sources.

Enrich a logon summary with GeoIP data to surface foreign source countries and ASNs for each summarized logon event.

```
$ hayabusa logon-summary -d ./evtx/ -G ./GeoIP/ -o logon-summary.csv
```

— Names flag, new columns, and event IDs with an example command. v4.1.0

03 **Expanded PowerShell coverage in extract-base64** IMPROVED

75

`extract-base64` now scans PowerShell event IDs `4100` and `4102` (Microsoft-Windows-PowerShell/Operational and PowerShellCore/Operational) and classic Windows PowerShell events `403` / `600`, checking the `ContextInfo` and Payload fields for `4100` / `4102` and `EventData.Data` detail blocks for `403` / `600`.

— Names exact event IDs and fields but no usage example. v4.1.0

THINNER COVERAGE BELOW

04 **Linux ARM64 musl release binary** NEW

50

Adds a Linux aarch64 (ARM64) musl release binary (`hayabusa-<ver>-lin-aarch64-musl`), built with a correct aarch64 musl cross-toolchain.

— Names the binary artifact but little else to act on. v4.1.0

05 **Embedded VERSIONINFO metadata in Windows binaries** IMPROVED

50

Windows executables now embed `VERSIONINFO` metadata (product name, file description, company name, copyright, original filename), with file and product versions auto-generated from `Cargo.toml`.

— Describes embedded fields but offers no user action. v4.1.0

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

NETRESEC

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

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

> NetResec's PolarProxy gains an outbound SOCKS proxy client for routing decrypted traffic (e.g. through Tor), a set of connection-timeout controls, and environment-variable configuration support.

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

01 **Outbound SOCKS proxy client via --connect** NEW 88

PolarProxy adds an outbound SOCKS proxy client using `--connect socks5:<host>:<port>` (or `socks4:<host>:<port>`), supporting both SOCKS4 and SOCKS5, enabling use cases such as routing inspected TLS traffic through Tor. For example, `PolarProxy --socks 1080 --connect socks5:127.0.0.1:9050 --nontls allow --pcapoverip 57012 --writeall` intercepts and decrypts HTTPS traffic before it exits through Tor, capturing all proxied traffic (including non-TLS) to a PCAP-over-IP stream for live analysis.

Intercept and decrypt HTTPS traffic before it exits through the Tor network, capturing all proxied traffic (including non-TLS) to a PCAP-over-IP stream for live analysis.

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

— Names exact flag, protocols, and a runnable command changelog-20260913-0f1a6645

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Chainguard

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

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

> Chainguard shipped a deployment-time FIPS-selectable Go/OpenSSL image, bumped Go to 1.27 across its Go image line, integrated Chainguard Libraries with JFrog Catalog, and added 39 new container images including a set of Kubeflow Pipelines FIPS variants.

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

01 go-openssl-fips deployment-time FIPS selection NEW

72

The new `go-openssl-fips` container image selects its FIPS-validated cryptographic module at deployment time rather than at compile time, letting a single artifact satisfy both OpenSSL FIPS and Go Cryptographic Module requirements without recompilation.

— Clear mechanism and named image, no usage example given. changelog-20260913-a78f20e2

02 39 new container images including Kubeflow Pipelines FIPS variants

NEW 63

Adds 39 new container images including 10 `kubeflow-pipelines-*` FIPS variants (`kubeflow-pipelines-api-server-fips` , `kubeflow-pipelines-cache-deployer-fips` , `kubeflow-pipelines-cache-server-fips` , `kubeflow-pipelines-driver-fips` , `kubeflow-pipelines-frontend-fips` , `kubeflow-pipelines-metadata-envoy-fips` , `kubeflow-pipelines-metadata-writer-fips` , `kubeflow-pipelines-persistenceagent-fips` , `kubeflow-pipelines-scheduledworkflow-fips` , `kubeflow-pipelines-viewer-crd-controller-fips`) plus `dbmate` , `hadolint` , `jruby` , `gubernator` , `fortiotel` , `packer` , `security-profiles-operator` , `opentelemetry-go-instrumentation` , `redpanda-console-fips` , and others.

— Names all listed images but no usage or mechanism given. changelog-20260913-a78f20e2

03 JFrog Catalog integration for Chainguard Libraries NEW

62

Chainguard Libraries integrates with JFrog Catalog, allowing joint customers to pull Chainguard-built packages through JFrog and enabling JFrog Zero-Touch Remediation to substitute patched Chainguard packages without changing developer workflows. Java support ships now, with JavaScript and Python to follow by end of September 2026.

— Explains mechanism and rollout timeline but no config/API named.

changelog-20260913-a78f20e2

THINNER COVERAGE BELOW

04 **Go 1.27 across Go container images** IMPROVED 50

Ships Go 1.27 across three Chainguard container images: `go`, `go-fips`, and `go-openssl-fips`.

— Names exact images and version but no further detail. changelog-20260913-a78f20e2

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SOAR

Tines

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

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

> Tines' 43.2.0 release expands the Cases workspace with API-driven field updates, priority labels and comment notifications, adds a new Cases surface to the Tines MCP for AI-driven workflows, and introduces change control comments, audit log retention configuration, formula-driven AI provider URLs, and dashboard draft mode.

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

01 **Cases workspace field API, priority labels, notifications** NEW 57

Tines added the ability to Update case fields via the API, enabling programmatic updates to case fields through the Tines API. The cases list view now surfaces priority labels for at-a-glance triage, and users receive case notifications when comments on a case are updated.

— Names the case field API and UI additions but no exact endpoint or field list.

changelog-20260913-03d32e8a

02 **Cases tools in Tines MCP** NEW 40

Tines MCP (Model Context Protocol) now includes Cases tools, exposing case management surfaces so AI-driven workflows can interact with cases.

— Names the MCP surface but not specific tool calls or schemas.

changelog-20260913-03d32e8a

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

Teams can now configure how long audit log data is retained.

— States the setting exists but not the config key or default value.

changelog-20260913-03d32e8a

04 **Change control comments** NEW 33

Reviewers can now add comments to annotate change control submissions.

— Describes the capability without a UI path or endpoint. changelog-20260913-03d32e8a

05 **Formula-driven AI provider URLs** NEW 25

AI provider URLs can now be set via formulas rather than static values, per the 43.2.0 changelog summary.

— Only named in the release summary, no mechanism or example given.

changelog-20260913-03d32e8a

06 **Dashboard draft mode** NEW 25

Dashboards gained a draft mode, per the 43.2.0 changelog summary.

— Only named in the release summary, no workflow detail provided.

changelog-20260913-03d32e8a

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL?

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

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

runZero is a cloud-based asset discovery and inventory platform that identifies and maps all connected devices across networks without agents.

> runZero's latest release focuses on tightening API access control with granular custom roles, while also improving asset visibility and task management in the UI, alongside a notable change to hostname discovery behavior.

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

01 **Custom roles for API keys and MCP connections** NEW

50

Account-level API clients can now use granular authentication scopes in addition to predefined roles, with permissions capped by the creator's own access rights. Custom roles are also being extended to MCP connections.

– Explains scope mechanism but no exact flag or endpoint named

changelog-20260913-24eeaafc

02 **NetBIOS hostname fallback removed** BREAKING

50

Hostname discovery no longer falls back to NetBIOS domains — assets that previously resolved hostnames via NetBIOS domain fallback will no longer do so, changing hostname resolution behavior for affected assets.

– States before/after behavior clearly but no migration steps changelog-20260913-24eeaafc

03 **Sub-asset visibility** NEW

15

runZero adds visibility into sub-assets, per the release summary; no further mechanism or UI detail is given.

– Only named in summary, no detail provided changelog-20260913-24eeaafc

└──▷ **BREAKING ON UPGRADE**

! Hostname discovery no longer falls back to NetBIOS domains — assets that previously resolved hostnames via NetBIOS domain fallback will no longer do so.

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

ConductorOne

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

RANK

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

> ConductorOne's latest release centers on AI agent governance with new call-time classifiers, alongside a guided MCP server registration flow, finer-grained access request controls, and two breaking changes to automation expressions and finding field names that API and SIEM consumers must account for.

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

01 **SSO handling of OIDC silent/fresh and SAML passive requests**

IMPROVED 55

SSO applications now honor OIDC silent and fresh authentication requests, and SAML passive requests, returning an error instead of silently reusing a session when a request cannot be completed safely.

– Names the exact protocol request types affected and new error behavior.

changelog-20260913-87306871

02 **Manual deprovisioning routing for revoke failures** IMPROVED

50

Revokes on connectors that cannot deprovision a given entitlement now route to manual deprovisioning instead of closing the task as Revoked while leaving the source unchanged.

– Explains before/after behavior for a specific failure case. changelog-20260913-87306871

03 **Full owner list toggle in app owner picker** IMPROVED

50

The app details page Edit owners picker adds an All users / Owners toggle so admins can see and manage the full owner list, including suspended or filtered-out users.

– Names the exact UI location and toggle. changelog-20260913-87306871

04 **Slack email-match account linking disabled** BREAKING

50

External Slack accounts (including Slack Connect members) can no longer be linked to a C1 user account by email match; notifications for affected users are skipped with a warning rather than silently bound.

— Explains removed behavior and new fallback but no migration steps.

changelog-20260913-87306871

05 **Bulk and individual finding reprocessing** NEW 45

Adds bulk and individual reprocessing of findings against current transformation and routing rules, with the option to keep or reset manual changes.

— Describes the mechanism but no UI path or API endpoint given.

changelog-20260913-87306871

06 **Entitlement binding within the same app** NEW 45

Adds entitlement binding support within the same app (e.g. Salesforce Admin -> Salesforce Editor) via the entitlement binding picker.

— Names the picker and an example pairing but no config surface.

changelog-20260913-87306871

07 **Duration limits surfaced in access request forms** IMPROVED 40

Duration limits are now shown up front in access request forms, suppressing the Indefinite option when a max is set and auto-adjusting invalid existing durations.

— Clear behavior change but no config key or UI path named. changelog-20260913-87306871

08 **Account suspension status in access request flows** IMPROVED 30

Access request flows now surface account suspension status for the target user or the holder of already-granted access.

— States the behavior with no further mechanism or location detail.

changelog-20260913-87306871

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

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

! The Owner column, filter, and detail field on findings are renamed Assignee. API consumers, webhook consumers, and SIEM integrations reading the Finding object or audit log must update to the new field and event names.

WAS THIS USEFUL? 👍 👎

Clerk

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

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

> Clerk added beta support for the OAuth 2.0 Device Authorization Grant, enabling authentication flows for browserless devices like CLIs, TVs, and game consoles.

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

01 **OAuth 2.0 Device Authorization Grant (beta)** NEW 76

Implements RFC 8628 Device Authorization Grant so applications that cannot open a browser or accept text input — CLIs, TVs, game consoles — can let users approve access from a separate browser-capable device. Supports both public clients (Client ID only) and confidential clients (Client ID + Client Secret), and automatically advertises `device_authorization_endpoint` and `urn:ietf:params:oauth:grant-type:device_code` in OAuth 2.0 and OpenID Connect metadata when the Device Authorization Grant is available and the verification page is reachable.

⋮

— Names spec, client types, and exact metadata fields; no code sample given.

changelog-20260913-8dea503f

WAS THIS USEFUL? 👍 👎

JumpCloud

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

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

> JumpCloud's biggest release of the window introduces Agent Identities as a non-human identity layer for AI agents alongside a new Password Vault and GA'd Access Risk Detection, while also adding a natural-language Custom Query Builder for reports, MCP usage discovery, SCIM mapping improvements, third-party MDM device trust, and Self Service App Catalog GA.

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

01 Agent Identities for AI agents (Public Preview) NEW

90

Introduces Agent Identities (Public Preview) under `Identity Management > Agents` for managing AI agents as non-human identities, with OAuth-based authentication via the JumpCloud AI Gateway and group-based access control through `Identity Management > Agent Groups`. Existing AI Gateway MCP servers created without an associated SSO application or bookmark must now have one assigned, since access is not scoped by User Groups until an application is assigned.

Register an AI agent identity and issue it OAuth credentials so it can authenticate to the JumpCloud AI Gateway 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.

— Names exact menu paths, auth mechanism, and a documented breaking caveat.

changelog-20260913-6fcef65f

02 SCIM group management and mapping UI IMPROVED

70

Expands SCIM group management for prebuilt and custom SCIM applications with a dedicated mapping UI for name overrides, extended schema mapping, side-by-side object transformation preview, and custom activation validation with selectable test users and groups, logging all sync rules to Directory Insights.

— Names several concrete mapping mechanisms but no exact navigation or command.

changelog-20260913-6fcef65f

03 Password Vault across portals and mobile NEW

60

Introduces Password Vault across Admin Portal, User Portal, JumpCloud Protect mobile app, and JumpCloud Go browser extension, enabling credential sharing, autofill, and bulk CSV/Excel import.

– Lists surfaces and capabilities but no config or command detail.

changelog-20260913-6fcef65f

THINNER COVERAGE BELOW

04 **Self Service App Catalog reaches GA** IMPROVED 55

Self Service App Catalog reaches GA, letting users install and manage JumpCloud App Catalog applications directly on macOS and Windows devices from within Software Management.

– Names the feature location but gives no setup or command detail.

changelog-20260913-6fcef65f

05 **Event-frequency triggers for Insights Rules** IMPROVED 45

Adds alert trigger conditions based on event frequency to Insights Rules, allowing threshold-based alerting instead of per-event firing.

– Describes the behavior change but no concrete threshold values or steps.

changelog-20260913-6fcef65f

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

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

WAS THIS USEFUL? 👍 👎

1Password

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

All the latest releases from the 1Password team

> 1Password rolled out full passkey support across its browser extension and native apps, letting users create, manage, and share passkeys everywhere, while Watchtower now helps identify logins ready to upgrade.

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

01 Passkey support in browser extension and apps NEW

62

1Password now supports creating, saving, and authenticating with passkeys directly in the browser extension across Chrome, Firefox, Edge, Brave, and Safari for sites that support passkey login. Saved passkeys can also be viewed, edited, moved, deleted, and shared from the native apps on Mac, iOS, Windows, Android, and Linux.

.
.
.
.

— Names platforms and browsers but no config or command detail

changelog-20260913-a09dc10e

THINNER COVERAGE BELOW

02 Watchtower flags passkey-upgrade-eligible logins NEW

40

Watchtower now flags existing saved logins that are eligible to be upgraded to a passkey, so users can review the list and create a passkey for each flagged site via the browser extension.

Identify which saved logins in your vault can be upgraded to a passkey without manually reviewing each site.

> 📍 In 1Password, open Watchtower. Review the list of logins flagged as passkey-eligible, then visit each site to create and save a passkey via the browser extension.

— Clear starting point via Watchtower UI but no further mechanism given

changelog-20260913-a09dc10e

WAS THIS USEFUL? 👍 👎

Didit

Feedback

2 RELEASES · SEEN 2026-09-13

CHANGELOG ↗

RANK

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

> Didit's ID Verification step gains non-document identity checks — national ID-number lookups and digital wallet sign-in — with per-country controls, configurable failure fallbacks, and matching support across the mobile SDKs and console sandbox, while the AML Screening node gets flexible entity-field mapping for non-standard documents.

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

01 **Non-document national ID lookup and digital ID wallet support**

NEW

90

Adds non-document national ID-number lookup: the user submits their national ID number and personal details, checked against an authoritative source (government register, credit bureau, or similar) with no photo or upload required. Per-country method controls are configurable via the Countries tab on the ID Verification step (and the API) to enable or disable document capture, national ID lookup, and digital ID wallets country by country. Fallback behaviour is configurable per failure mode — partial match, no match, no source response, or cancelled/timed-out wallet sign-in — each routing the user to document capture or declining the session. Lookup retry count is configurable from one to five attempts (default two), with only source-answered attempts counted toward billing and format-invalid numbers never reaching the source. Digital ID wallet support is on the roadmap for MitID, BankID, itsme, Vipps, iDIN, UAE PASS, gov.br, and EUDI Wallet, configurable in the console as Coming soon but not yet enabled for production; sandbox applications can already test every wallet in the catalog with simulated results independent of production availability. Mobile SDKs 4.8.0 (iOS, Android, React Native, Flutter) surface national ID lookup and digital ID wallet sign-in on a single entry screen alongside document capture, with on-device field validation before submission.

Enable national ID-number lookup for a specific country so users in that country can verify without uploading a document — useful when reducing drop-off in markets with high government-register coverage.

📍 In the Didit console, open your workflow, select the ID Verification step, go to the Countries tab, find the target country, and toggle Non-document lookup on. Configure the failure-mode switches (partial match, no match, no source response) to either fall back to document capture or decline the session, then save.

Upgrade the Web SDK to 4.8.0 to pick up the non-document lookup flow and the corrected `SDK_VERSION` constant in your CI pipeline.

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

— Names config surfaces, wallet list, retry limits and console steps

changelog-20260913-1233caae | snapshot-20260913

---

02 **Screened entity mapping in AML Screening node** NEW

80

Adds a Screened entity tab to the AML Screening node so practitioners can map screening inputs (name, date of birth, country, document number) directly from Document AI fields, questionnaire answers, `expected_details`, or `metadata` — enabling AML screening on flows using non-standardised documents such as tax certificates or notarised incorporation deeds, without an ID Verification or KYB Registry step. Adds an Entity type selector to screen either a `person` or `company`, routing company searches against company records, and an Incomplete screening data control (default Review, with a No action option) for flows that knowingly hold only partial identity data.

When your AML screening flow is built around a Document AI step (e.g. a notarised deed) rather than an ID Verification step, configure the Screened entity tab to pull identity fields — including the automatically-detected `full_name` — into the screening node.

> 📍 In the workflow console, select your AML Screening node › open the Screened entity tab › set Entity type to person › under Field sources, map name to your Document AI field (e.g. full_name), date of birth to dob, and country to country_of_issue › set Incomplete screening data to Review › publish the workflow.

— Names tab, selector and control with exact console steps product docs

---

03 **Verification method and assurance tier on webhooks and decision API**

NEW

60

Adds `status.updated` webhook and decision API fields carrying the verification method (Documentary , Data match , Cryptographic) and assurance tier for every ID Verification session.

— Names webhook and field values but gives no usage example changelog-20260913-1233caae

THINNER COVERAGE BELOW

04 **SDK_VERSION constant in Web SDK package** NEW

45

Adds `SDK_VERSION` constant to `@didit-protocol/sdk-web`, generated from the package version across all build formats and the TypeScript declaration.

Upgrade the Web SDK to 4.8.0 to pick up the non-document lookup flow and the corrected `SDK_VERSION` constant in your CI pipeline.

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

— Names constant and package but minimal explanation of use `changelog-20260913-1233caae`

05 **Embedded mode sizing in Web SDK** IMPROVED 40

Embedded mode in the Web SDK now uses the host element's content box instead of inheriting the modal height cap.

— Describes the behaviour change but no example or config key `changelog-20260913-1233caae`

06 **Specific rejection reason on questionnaire failure** IMPROVED 30

Surfaces the server-provided rejection reason to users when a questionnaire submission fails, replacing the previous generic error message; the mobile SDKs also adopt this improved questionnaire error messaging.

— States the before/after but no named surface or example `snapshot-20260913`

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ 1 RELEASE · 2026-09-12 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's v4.0.2 release adds AI-driven workflow steps, full TPRM data support in domain export/import, a unified PDF report engine, and a batch of smaller UI, filtering and localization improvements.

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

01 **Folder-level `is_published` field** NEW 65

A new `is_published` field, controlled at the Folder level, manages publication state for folder-level objects.

– Names the exact field and its scope for direct use v4.0.2

02 **TPRM data in domain export/import** IMPROVED 60

Domain export/import operations now carry the full TPRM (third-party risk management) data set, so third-party risk records travel with other domain data during export/import.

– Clear scope but no exact command or endpoint named v4.0.2

THINNER COVERAGE BELOW

03 **Bulk import of applied controls and owners** IMPROVED 55

The data-wizard now supports importing applied controls and owners together with findings, enabling richer bulk data intake in a single operation.

– Names data-wizard and the imported entities together v4.0.2

04 **Quick-add custom metric sample** NEW 50

A new context menu action lets users quickly add a `custom-metric-sample` directly from the UI.

– Names the exact object type added via UI action v4.0.2

05 **Unified PDF report rendering engine** IMPROVED 50

PDF report exports are now unified under a single new rendering engine, producing a consistent layout across all report types.

— Explains mechanism but no format/version specifics v4.0.2

06 **AI call support in workflows** NEW 45

Workflow definitions can now include AI-driven steps via new AI call support, enabling automated AI-driven steps within CISO Assistant workflow definitions.

— Names the capability but no config/flag detail given v4.0.2

07 **Date filters across the platform** NEW 40

Date filters have been added across the platform, allowing users to narrow object lists by date ranges.

— Prose description, no specific fields or UI path named v4.0.2

08 **Requests management via quick forms** NEW 40

A new requests management system is accessible through quick forms, enabling streamlined intake of requests.

— Names the feature but not the underlying form/config v4.0.2

09 **Audit table-mode rework** IMPROVED 35

The audit table-mode in the frontend has been reworked with an updated layout and interaction model.

— Describes change but no specifics on new interactions v4.0.2

10 **German NIS2 ENISA translations** NEW 35

German NIS2 ENISA translations have been added to the framework library.

— Simple addition with no further mechanism described v4.0.2

WAS THIS USEFUL?  

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

Obsidian

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

The free and flexible app for your private thoughts.

> Obsidian's 1.14.1 update focuses on small quality-of-life additions: configurable Quick Capture widget locations on iOS, OpenStreetMap templates, an updated math renderer, and right-to-left support in Bases tables.

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

01 **Accessibility text scaling CSS variable** NEW 70

Themes and snippets can override text scaling for specific elements to respect the user's mobile accessibility text size preference using the `--font-preferred-size` CSS variable, e.g. `.my-element { font-size: var(--font-preferred-size); }`.

Override text scaling in a theme or snippet so specific elements respect the user's accessibility text size preference on mobile.

```css
.my-element {
  font-size: var(--font-preferred-size);
}
```

– Names exact CSS variable and shows runnable snippet changelog-20260913-0c58d438

THINNER COVERAGE BELOW

02 **iOS Quick Capture widgets can target a Location** IMPROVED 50

The iOS Lock Screen and Control Center Quick Capture widgets can now be configured to open a specific Location, rather than only a fixed default capture target.

– Explains the change but no config path or steps given changelog-20260913-0c58d438

03 **MathJax updated to 4.1.3** IMPROVED 25

The bundled MathJax math rendering library was updated to version 4.1.3.

– Version number given but no behavioural detail changelog-20260913-0c58d438

04 **OpenStreetMap templates** NEW 15

Obsidian 1.14.1 adds OpenStreetMap templates, per the release summary; no further detail on scope or usage was provided.

— Mentioned only by name in the summary `changelog-20260913-0c58d438`

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 13, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ **Subscribe** Feedback on this issue