THE CYBER TOOLCHAIN

NO. 051

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 20, 2026 · EVERY DAY

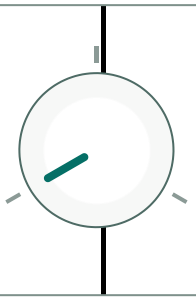
The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // **CONTENTS** SHOW 13 tools

APPLICATION SECURITY

vim ? help

◆ SAST / SCA / Code Security

StackHawk

Feedback ⓘ 1 RELEASE · SEEN 2026-08-19 NOTES ↗

StackHawk is an application security testing platform that performs dynamic security scanning to find vulnerabilities in web applications during development and CI/CD pipelines.

> StackHawk added in-place Team ownership management for applications with broader visibility for Members and View Only users, shipped a `wingman` skill bundle for GitHub Copilot, added new team-availability API endpoints, and fixed a bug where the PUT team-application endpoint silently failed to save assignments.

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

01 **Wingman plugin bundle for GitHub Copilot** NEW 92

Introduces `wingman`, a StackHawk umbrella plugin for GitHub Copilot that bundles four skills — `hawkscan`, `stackhawk-api`, `data-seed`, and `optimize` — in one install, since Copilot has no plugin-dependency resolution mechanism. Adds a separate `hawkscan-ci` skill installable via `copilot plugin install hawkscan-ci@stackhawk` for CI-focused scanning. Plugins installed via `copilot plugin install` are stored in `~/.copilot/installed-plugins/` and available across all projects, with additional project-skill directories configurable via the `chat.agentSkillsLocations` setting; the same marketplace catalog now also serves Claude Code and Codex.

Install the full StackHawk skill set for GitHub Copilot, then add the CI scanning skill separately.

```
$ copilot plugin install wingman@stackhawk
copilot plugin install hawkscan-ci@stackhawk
```

— Names every skill, config setting, storage path and a runnable install command

product docs

02 **Team assignment endpoint now saves correctly** BREAKING 85

`PUT /api/v1/org/{orgId}/team/{teamId}/application` previously returned a success response without actually saving the Team assignment. It now saves correctly, but any application-to-Team assignments made through that endpoint before the fix must be re-run to confirm they are actually in place.

— Exact endpoint and before/after behavior with a clear migration action

snapshot-20260819

03 **Team ownership management for applications** NEW 82

Adds a Team ownership column to the Applications table letting users change a Team assignment in place; applications without a Team are marked `Unassigned` and can be assigned by selecting the label and searching for a Team. Adds a matching Team field in `Application Settings > General` (with `Unassigned` at the top) so clearing or changing ownership works the same way in both places, and moving an application between Teams no longer requires removing it from its current Team first. Members can now open Teams they belong to and View Only users can review every Team in the organization without manage permissions. Team management controls (Create a Team, Add Members, Add Applications, rename, Delete Team) are shown disabled rather than hidden for users without manage permissions. In the Create Application flow, users who cannot manage Teams but belong to at least one Team must now assign the new application to one of their Teams, and the `Filter by Unassigned Applications` checkbox now returns results for Members and View Only users.

— Full UI mechanism and permission scope named, no exact API tied to it snapshot-20260819

THINNER COVERAGE BELOW

04 **New team availability endpoints** NEW 45

Adds `GET /api/v1/org/{orgId}/teams/available/applications` and `GET /api/v1/org/{orgId}/teams/available/users` endpoints to the API.

— Endpoints named but no description of behavior or use case 0.0.1

└──▷ **BREAKING ON UPGRADE**

! `PUT /api/v1/org/{orgId}/team/{teamId}/application` previously returned a success response without saving the Team assignment; it now saves correctly. Any application-to-Team assignments made through that endpoint must be re-run to confirm they are actually in place.

! The `PUT /api/v1/org/{orgId}/team/{teamId}/application` endpoint previously returned a success response without saving the Team assignment; assignments made through this endpoint were silently dropped and must be re-submitted to take effect.

WAS THIS USEFUL? 👍 👎

GitHub

Feedback ⓘ 1 RELEASE · 2026-08-19 BLOG ↗

GitHub is a web-based platform for version control and collaborative software development using Git repositories.

> GitHub shipped CodeQL 2.26.3, adding new taint-flow models for JavaScript/TypeScript, Vue, Sails, and C/C++, tightening several GitHub Actions security queries, and removing a deprecated query module.

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

01 GitHub Actions query accuracy improvements IMPROVED

80

GitHub Actions analysis now recognizes untrusted data in `github.event.merge_group` for workflows triggered by the `merge_group` event. The `js/missing-rate-limiting` query now recognizes `@fastify/rate-limit` as a rate limiter. `actions/output-clobbering/high` no longer reports simple `jq` path filters when their output remains JSON-encoded. `actions/cache-poisoning/poisonable-step` and `actions/untrusted-checkout/critical` now start alert paths at the expressions that control untrusted checkouts. `actions/envvar-injection/critical` now requires the untrusted source and privileged context to originate from the same trigger event, and no longer treats pull request head labels as injection-capable. `actions/cache-poisoning/code-injection`, `actions/cache-poisoning/direct-cache`, and `actions/cache-poisoning/poisonable-step` now account for read-only cache access on low-trust triggers running in the default branch scope. Queries also now correctly classify the `schedule` event when determining whether a workflow can be externally triggered.

— Names each affected query id and exact behavior change

CodeQL 2.26.3 improves GitHub Actions q…

02 New taint-flow models across languages NEW

74

Adds `file:<path>` package name syntax for JavaScript/TypeScript custom models, letting analysts define sources and sinks from a file's public exports. Adds flow models for Vue Composition API helpers `ref`, `shallowRef`, `toRef`, `reactive`, and `computed`, and recognizes Vue Router's useRoute() as a client-side remote flow source including its `query`, `params`, `path`, `fullPath`, and `hash` members. Treats declared `inputs` properties in Sails Action2 controller files as remote flow sources, potentially improving `js/path-injection` results, and tracks promise-wrapped client response data into promise fulfillment values under the response threat model, potentially improving `js/xss` results. Also adds flow source models for `RegQueryValue` and related functions from the `winreg.h` Windows header in C/C++.

— Names exact APIs and affected queries but no runnable steps

CodeQL 2.26.3 improves GitHub Actions q…

THINNER COVERAGE BELOW

03 **SelfHostedQuery module removed** BREAKING 55

The `codeql.actions.security.SelfHostedQuery` module has been removed; any custom queries that import or rely on this module must be updated.

— Names exact module but gives no migration path CodeQL 2.26.3 improves GitHub Actions q…

04 **Ruby vendored gem taint source removed** IMPROVED 30

Removes Ruby library input to vendored gems from the set of taint sources, reducing false positives when using vendoring.

— Brief mention with no query or example named CodeQL 2.26.3 improves GitHub Actions q…

└──▷ **BREAKING ON UPGRADE**

! The `codeql.actions.security.SelfHostedQuery` module has been removed; any custom queries that import or rely on this module must be updated.

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

DataDome

Feedback ⓘ 1 RELEASE · 2026-08-20 BLOG ↗

DataDome is a bot management and API protection platform that defends applications against automated attacks and fraud using AI-driven detection.

> DataDome's iOS Alamofire SDK now automatically merges its bot-detection cookie with cookies manually added to requests, removing a manual step for developers.

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

01 Automatic cookie merging in Alamofire SDK IMPROVED

55

The iOS SDK for Alamofire (4.1.0) automatically merges the DataDome cookie with cookies manually added to a request inside `DataDomeInterceptor` instances, so developers no longer need to manually combine them.

— Names the interceptor class but not full mechanism or migration steps.

iOS SDK for Alamofire 4.1.0 (2026-08-20)

WAS THIS USEFUL? 👍 👎

caido

Feedback

1 RELEASE · 2026-08-20

NOTES ↗

Caido releases, wiki and roadmap

> Caido v0.58.0 adds race-condition testing through a new Replay Pipeline session type, extends HTTPQL with dedicated header and body fields, and reworks the Plugin page and sidebar for better navigation.

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

01 **HTTPQL header and body fields** NEW 83

HTTPQL gains `req.header`, `req.header["<name>"]`, `req.body`, `resp.body`, and `resp.header` fields, letting queries target specific headers or body content without scanning the full `raw` field; all support `.eq`, `.cont`, and `.regex` operators.

Isolate Bearer token headers or sensitive body patterns in HTTP history without false positives from the rest of the raw request.

```
$ req.header["Authorization"].cont:"Bearer" and
req.body.regex:"password=[^&]+"
```

— Names exact fields and operators with a working query example. v0.58.0

02 **Replay Pipeline sessions for race-condition testing** NEW 80

A new Pipeline Replay session type supports race-condition testing with two strategies: Sequential (ordered execution) and Last Byte Synchronization, which holds back the final byte of every request and releases them all simultaneously.

Test a login endpoint for race conditions by synchronising the final byte of multiple requests so they arrive at the server simultaneously.

> 📍 In Replay, select New Session › Pipeline, add the target requests, choose the Last Byte Synchronization strategy, then click Run.

— Explains both strategies and gives exact UI steps to run one. v0.58.0

03 **Reworked Plugin page** IMPROVED 60

The Plugin page now shows an Official badge, quality rating, author, download count, and version per plugin, and supports filtering by Official or Community and bulk install/update.

— Lists concrete new metadata and controls but no exact navigation given. v0.58.0

THINNER COVERAGE BELOW

04 **Customizable sidebar** NEW 45

The sidebar can now be reordered via drag-and-drop, items can be pinned or hidden, and users can create custom categories for pages and plugins.

— Describes mechanism but no exact config or command given. v0.58.0

05 **Command palette 'Go to' navigation** NEW 28

Pages and plugins are now reachable via a `Go to` entry in the command palette.

— Thin one-line description with no further detail. v0.58.0

06 **Multiple commands per shortcut** IMPROVED 20

The same keyboard shortcut can now be assigned to multiple commands simultaneously.

— Bare statement with no configuration detail. v0.58.0

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

PCAPdroid

Feedback ⓘ 1 RELEASE · 2026-08-19 CODE ↗

No-root network monitor, firewall and PCAP dumper for Android

> PCAPdroid v2.0.0 adds a Capture List screen, per-app traffic isolation, settings export/import, and port mapping exemptions, while bumping its mitm and ushark decryption modules and raising minimum Android version requirements.

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

01 **mitm addon updated with new Android requirements** BREAKING

70

Bumps the mitm addon to v2.3 (mitmproxy 12.2.3) with full 16 KB page-size device support; the mitm addon now requires Android 24+ and drops support for the x86 and armeabi-v7a ABIs.

– Names exact versions and dropped ABIs, a clear compatibility note. v2.0.0

THINNER COVERAGE BELOW

02 **Packet direction persisted via pcapng EPB flags** IMPROVED

55

Persists packet direction in root mode via the pcapng EPB flags option.

– Names the exact pcapng mechanism used, scoped to root mode. v2.0.0

03 **Per-app allowlist (app isolation)** NEW

45

Implements per-app allowlist (app isolation) to restrict which apps' traffic is captured.

– Describes purpose but not the setup steps. v2.0.0

04 **Port mapping exemptions** NEW

45

Adds port mapping exemptions to exclude specific ports from VPN port remapping.

– Explains mechanism but no config location given. v2.0.0

05 **Capture List screen for past captures** NEW

40

A new Capture List screen shows past captures and their size on disk.

– Names the screen but no navigation path or storage details. v2.0.0

06 **New UI translations added** NEW

40

Adds new UI translations: Bengali (BN), French (FR), Hindi (HI), Japanese (JA), Korean (KO), Malay (MS), Urdu (UR), Vietnamese (VI).

— Lists all languages added but no other detail. v2.0.0

07 **Minimum Android version raised to 23** BREAKING 40

PCAPdroid now requires Android 23+ (minSdk raised to 23); devices running Android 22 or below are no longer supported.

— Clear before/after but no migration guidance beyond the cutoff. v2.0.0

08 **Settings export and import** NEW 35

Adds settings export and import for backing up and restoring PCAPdroid configuration.

— Bare feature description with no file format or menu path. v2.0.0

09 **ushark decryption module bumped to Wireshark v4.7.1** IMPROVED 30

Bumps ushark decryption module to Wireshark v4.7.1.

— Version number given but no behavioural change described. v2.0.0

10 **pcapng format implicitly enables extensions** IMPROVED 30

Implicitly enables PCAPdroid extensions when using the pcapng capture format.

— States trigger condition but not which extensions are enabled. v2.0.0

11 **Android 17 / Target SDK 37 support** IMPROVED 30

Adds Android 17 (Target SDK 37) support.

— Named target SDK version but no behavioural detail. v2.0.0

12 **Configurable connection log size** IMPROVED 20

Makes the connections log size configurable.

— No default, limit, or setting name provided. v2.0.0

└──▷ **BREAKING ON UPGRADE**

! PCAPdroid now requires Android 23+ (minSdk raised to 23); devices running Android 22 or below are no longer supported.

! The mitm addon now requires Android 24+ and drops support for the x86 and armeabi-v7a ABIs.

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Plerion

Feedback ⓘ 1 RELEASE · 2026-08-20 NOTES ↗

Plerion is a cloud security platform that enables continuous vulnerability discovery and remediation across cloud infrastructure and applications.

> Plerion brought detection exemptions to the API, letting teams read, write, and clear exemptions programmatically with immediate re-evaluation of affected findings.

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

01 **API access to detection exemptions** NEW 69

New API endpoints let teams read, write, and clear detection exemptions on any detection without opening the platform UI. Exemptions can match on asset name, tags, region, principal, or API Gateway route, and existing findings on the dashboard are re-evaluated immediately when an exemption is written rather than waiting for the next scan. Plerion also notes that teams should list profiles via the API first, since the default profile only covers integrations that don't have a profile of their own.

— Describes matching criteria and behaviour but no endpoint paths given

Detection exemptions, now over the API:

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Iru

Feedback ⓘ 5 RELEASES · 2026-08-19 NOTES ↗

> Iru shipped new Android Restrictions Library Item controls for credential managers and managed Google Accounts, exposed iOS/iPadOS hardware health statuses in device records and the enterprise API, added version pinning for Mac Auto Apps, and gave Identity directory sync integrations configurable sync frequency plus on-demand refresh.

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

01 Hardware health statuses for iOS/iPadOS devices NEW

73

Exposes device system health statuses for hardware components (camera, NFC, baseband, Touch ID, and others) in the device record UI for supported devices running iOS or iPadOS 27 beta, and makes those values available via the enterprise API device details endpoint for iOS and iPadOS devices.

– Names components, UI, and API surface but no exact endpoint path

Device health statuses for iOS and iPad…

02 Configurable sync frequency and on-demand sync for directory integrations

NEW

71

Adds configurable sync frequency per directory sync integration, with intervals including Manual Only, Every 30 minutes, every hour, 2 hours, 4 hours, 8 hours, 12 hours, daily, every 2 days, or weekly, plus a Refresh and Sync Now capability for directory sync integrations.

– Lists exact intervals and controls but no config path or endpoint

Iru Identity Directory Sync Enhancements

03 Credential manager and Google Account controls in Android Restrictions

NEW

65

Adds a Credential managers setting to the Android Restrictions Library Item, letting admins block all credential managers or allow the device's pre-loaded system credential managers in the work profile on managed Android devices. Also adds a managed Google Account setting to the same Library Item, with two modes controlling which managed Google Accounts are permitted on company-owned Android devices with work profiles.





— Names the exact settings but not the two Google Account modes in detail

Require a managed Google Account on And… | Control credential managers on Android …

04 **Pin specific version for Mac Auto Apps** NEW 60

Mac Auto Apps now support enforcing a specific version, selectable from a list of Iru-hosted versions, so devices installing for the first time or that are out of date install the pinned version rather than the latest available.



— Explains behavior and selection but no config key or command

Enforce a specific version for Mac Auto…

WAS THIS USEFUL? 👍 👎

Trend Vision One

Feedback ⓘ

2 RELEASES · 2026-08-10 → 2026-08-20 BLOG ↗

Trend Vision One is Trend Micro's unified cybersecurity platform providing threat intelligence, vulnerability management, and incident response across endpoints and networks.

> Trend Vision One let IR teams pull Forensics evidence directly into Workbench insight timelines, and shipped a Virtual Network Sensor update adding GTP, NSH, and Teredo protocol inspection with new CLI toggle commands.

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

01 GTP, NSH, Teredo protocol support in Virtual Network Sensor

NEW 71

Virtual Network Sensor 1.0.1737 adds decoding and inspection of GPRS Tunnelling Protocol (`GTP`), Network Service Header (`NSH`), and `Teredo` traffic, along with new CLI commands to enable and disable inspection for `GTP` , `NSH` , `Teredo` , `VXLAN` , and `VXLAN GPE` protocols.

— Names protocols and CLI commands but not exact syntax

Virtual Network Sensor version 1.0.1737…

02 Forensics evidence added to Workbench and Forensics timelines

NEW 70

From a Forensics evidence package, IR and SOC teams can select relevant evidence items and click `Add selected to Workbench insight timeline` to consolidate them into one shared chronological record for a Workbench insight. The same evidence selection workflow also supports adding selected evidence to a Forensics timeline.

Consolidate Forensics evidence into a Workbench insight timeline so IR and SOC teams share one chronological record without manually correlating separate sources.

> 📍 In Agentic SIEM and XDR → Forensics, open a Forensics evidence package, select the evidence items relevant to your investigation, then click `Add selected to Workbench insight timeline` .

— Exact button label and navigation given, but no API or config surface

Add Forensics evidence to a Workbench i…

WAS THIS USEFUL? 👍 👎

Microsoft Sysinternals

Feedback ⓘ 1 RELEASE · 2026-08-19

BLOG ↗

Microsoft Sysinternals is a suite of advanced system utilities for Windows diagnostics, monitoring, and troubleshooting at the kernel level.

> Sysinternals shipped updates across three utilities: a new IPC event class in Process Monitor, a macOS DemoMirror feature in ZoomIt, and restored Remote Desktop gateway support in RDCMan.

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

01 **IPC event class in Process Monitor** NEW 55

Process Monitor v4.1 adds an `IPC` event class, enabling real-time observation of named pipe and mailslot activity alongside the existing file system, Registry, and process/thread event classes.

– Names the event class but no exact UI steps to enable it

Process Monitor v4.1, ZoomIt 12.3 for m…

02 **DemoMirror in ZoomIt for macOS** NEW 47

ZoomIt 12.3 for macOS introduces DemoMirror, which mirrors the screen, a screen region, or a window onto a second monitor.

– Describes the feature's function but not how to invoke it

Process Monitor v4.1, ZoomIt 12.3 for m…

03 **RD gateway support restored in RDCMan** IMPROVED 25

RDCMan v3.21 re-enables Remote Desktop gateway support.

– Bare statement of restored support with no further detail

Process Monitor v4.1, ZoomIt 12.3 for m…

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Axonius

Feedback ⓘ 1 RELEASE · 2026-08-20 BLOG ↗

Axonius is a cybersecurity platform that discovers, manages, and secures all connected devices and users across enterprise networks.

> Axonius's biggest addition is a full Ingestion Rules engine — per-adapter conditions and post-ingest data transforms — introduced across three docs updates, alongside 9.0.5's OAuth 2.1 service-account auth, parallel adapter connection fetching, seven new adapters, and GitHub Advisory Database CVE enrichment.

└──▷ **WHAT SHIPPED · 18 FEATURES** most completely described first ? what's the number?

01 **Post actions for Ingestion Rules** NEW 95

Ingestion Rules gain post actions chained with `then`: `skip_field` removes named fields before they're written to the database (e.g. `device key_exists ["id"] then skip_field ["physical_location", "qualys_agent_ports"]`); `remove_values` drops matching values from list fields; `remove_items` drops entire list items when a subfield condition matches (e.g. `remove_items network_interfaces.ip4 in_net ["10.20.0.0/24"]`); `trim_prefix` / `trim_suffix` strip literal text and `trim_regex` strips a regex match (with (?i) for case-insensitivity); `set_value` creates or overwrites a field from static literals, field references, or transforms including `regex_extract` (capture-group index, default `1`), and automatically preserves any overwritten value in a new `<field>_original` field. Post actions can also use `key_exists` / `key_not_exists` conditions.

Drop PII fields (e.g., physical location and agent ports) from every device ingested by an adapter.

```
$ device key_exists ["id"] then skip_field ["physical_location", "qualys_agent_ports"]
```

Strip a MAC address suffix appended to EC2 hostnames so the `ad_hostname` field contains only the clean hostname.

```
$ device key_exists ["id"] then trim_regex ad_hostname ["-([A-Fa-f0-9]{2}(:[A-Fa-f0-9]{2}){5})"]
```

Extract the hostname from a device remote URL into a dedicated `host` field for easier querying and reporting.

```
$ device.remote_url key_exists ["id"] then set_value host =
regex_extract(device.remote_url, "https?://([^/]+)", 1)
```

— Every post action's syntax, mechanism, and edge cases are documented with runnable examples.

product docs

---

02 **Operator set for Ingestion Rules conditions** NEW 90

Documents the full operator set for primary Ingestion Rule statements: `==` / `!=` (with the caveat that `!=` only matches assets where the field exists, requiring `key_not_exists` for missing fields), date comparisons `<` / `>` via date(YYYY-MM-DD), date(now-nd), date(now+nd) (`>=` / `<=` unsupported for dates), numeric `<` / `>` / `>=` / `<=` , `in` / `not_in` , `in_net` / `not_in_net` (IPv4 and IPv6 CIDR), `starts_with` / `not_starts_with` , `ends_with` / `not_ends_with` , `key_exists` / `key_not_exists` , `field_equal` / `field_not_equal` , `field_starts_with` / `field_not_starts_with` , `contains` / `not_contains` (case-insensitive), and `match_regex` / `not_match_regex` .

Exclude low-confidence OS data during ingestion — skip OS fields for any device whose confidence score is below 65.

```
$ device.confidence_level < 65 then skip_field ["os.type",
"os.distribution", "os.type_distribution", "os.os_str"]
```

Filter ingestion to devices whose IP is inside a specific corporate subnet, using the `in_net` CIDR operator.

```
$ device.network_interfaces.ips in_net ["10.10.11.0/24"]
```

Ingest only active users by requiring last logon within the past 10 days, using a relative date expression.

```
$ user.last_logon > date(now-10d)
```

— Every operator named with exact syntax and behavioral caveats, backed by runnable examples.

product docs

03 **Ingestion Rules configuration and testing UI** NEW 90

Adds an `Ingestion Rules Configuration` page under each adapter's `Advanced Settings`, with a toggle to enable rules and a `Select logical operator for all rules` drop-down supporting `OR`, `AND`, or `Custom` (via a `Custom Logical Expression` field accepting expressions like 1 AND (2 OR 3), case-sensitive uppercase keywords). An `Enable ingestion rules settings for each connection separately` toggle adds an `Ingestion Rules Configuration` tab to the `Add Connection` drawer. A `Save and Fetch` action tests rules immediately, with results visible via `From Last Fetch - yes` in the Query Wizard and in `Adapter Fetch History`. Excluded entities remain until the `Delete devices (or users)...` retention window expires.

Apply a complex filter so only assets matching rule 1 AND either rule 2 or rule 3 are ingested from an adapter connection.

> 📍 In Adapters, open the adapter › Advanced Settings › Ingestion Rules Configuration. Toggle on 'Enable ingestion rules to configure which data to ingest from the adapter into the system'. Set `Select logical operator for all rules` to `Custom`. In the `Custom Logical Expression` field enter: 1 AND (2 OR 3). Click Save.

Configure different ingestion rules for each adapter connection, then immediately test them with a fetch.

> 📍 In Adapters, open the adapter › Advanced Settings › Ingestion Rules Configuration. Toggle on 'Enable ingestion rules settings for each connection separately'. Click Save. Then click Add Connection, select the `Ingestion Rules Configuration` tab, toggle on 'Enable ingestion rules to configure which data to ingest from the adapter into the system', configure the rules, and click `Save and Fetch`.

— Exact UI navigation, toggle names, and expression syntax given step by step.

product docs

---

04 **Parallel connection fetching for discovery** NEW 80

Adds a `Number of connections to fetch in parallel` field in Adapter Discovery Configuration, letting practitioners set simultaneous connection counts (1 up to the adapter's maximum, default 1/sequential) during scheduled discovery cycles; enabled for Claroty CTD, F5 BIG-IP iControl, Infoblox DDI, Salesforce, VMware ESXi, and vSphere adapters.

Speed up discovery for adapters with many connections by enabling parallel fetching in Adapter Discovery Configuration.

📍 In the Axonius console, go to the adapter settings for a supported adapter (e.g., Salesforce or VMware ESXi), open Adapter Discovery Configuration, and set 'Number of connections to fetch in parallel' to the desired concurrency value (e.g., 5).

— Named field, default value, range, and the specific adapters it applies to.

Axonius Release Notes 9.0.5 (2026-08-20)

---

05 **Advanced settings added across existing adapters** NEW

80

Adds per-adapter advanced settings: AppViewX CERT gets Enrich certificates with discovery data and a Discovery Name field for cipher, TLS version, and port scan enrichment; Cisco ASA gets a Connection Method setting to choose Legacy REST API or HTTP Interface (required for Firepower 2100/2120); Cisco Identity Services Engine gets API Gateway support routing through Layer7 or IBM API Connect; CrowdStrike Falcon's `CSPM Account / Tenants Settings` gains an OCI account type ingesting tenancy name, tenancy OCID, home region, user information, and CSPM Status; the Custom Files adapter gains Software asset fetching from CSV and JSON files, a configurable custom field delimiter (e.g. semicolon or pipe), and SMB Distributed File System (DFS) path support; Certero gets a Certificate advanced setting (enabled by default) to disable Certificate asset fetching; Azure Defender for IoT gets a MAC address parsing option for uncertain (Guess) MAC addresses.

— Every adapter-specific setting and its exact behavior is named.

Axonius Release Notes 9.0.5 (2026-08-20)

---

06 **CSV export for chart visualizations** NEW

75

Adds CSV export for all chart visualization types — Bar, Pie, Donut, Stacked Bar, Line, Table, and Venn — across all compatible widgets, including count and percentage values, a Total row, full numeric values, and filenames formatted as `Axonius - [Chart Name] - DD Month YYYY, HH.MM AM/PM.csv`.

— Names all chart types and exact filename format, no export trigger location given.

Axonius Release Notes 9.0.5 (2026-08-20)

---

07 **GitHub Advisory Database CVE enrichment** NEW

75

Adds enrichment of software vulnerability data from the GitHub Advisory Database, toggled via `Enrich software vulnerabilities from GitHub Advisory Database` in Settings > Enrichment > CVE Enrichment Settings, with a `Fetch GitHub Reviewed Advisories` option for curated coverage; supplements CVE data with CVSS v3/v4, EPSS, and exploit availability details.

Enable GitHub Advisory Database enrichment to supplement CVE data with CVSS v3/v4, EPSS, and exploit availability details for software vulnerabilities.

📍 In the Axonius console, go to Settings › Enrichment › CVE Enrichment Settings, toggle on 'Enrich software vulnerabilities from GitHub Advisory Database', then select Fetch GitHub Reviewed Advisories for curated coverage.

— Exact settings path and toggle names given, with concrete data fields enriched.

Axonius Release Notes 9.0.5 (2026-08-20)

08 **OAuth 2.1 authentication for service accounts** NEW

70

Adds OAuth 2.1 authentication for service accounts; access tokens are issued via the `/api/oauth2/token` endpoint and are automatically invalidated on credential reset or new token generation.

— Names the endpoint and invalidation triggers but not full auth flow.

Axonius Release Notes 9.0.5 (2026-08-20)

09 **Vault support for sensitive file fields** IMPROVED 65

Extends the Enterprise Password Manager (vault) integration beyond password fields to support sensitive file fields: client certificate files (`.pem`), client private key files (`.pem`), advanced configuration files (JSON/XML), and credentials-format files.

— Names each new supported file type but not the setup steps.

Axonius Release Notes 9.0.5 (2026-08-20)

10 **Seven new adapters added** NEW 65

Adds Black Duck Polaris (Aggregated Security Findings, Application Resources, Business/SaaS Applications), Cisco IoT Control Center (Devices), Invicti Platform Cloud (Aggregated Security Findings, Business/SaaS Applications, URLs), Mashery/Boomi Cloud API Management (Application Services, Business Applications, Organizational Units, Secrets, Security Roles, URLs, Users), Mindtickle (Groups, Users), Smart SD (Devices), and StrongDM (Devices).

— Every new adapter and its asset types are named.

Axonius Release Notes 9.0.5 (2026-08-20)

11 **Include-only mode for data scope field access** NEW

60

Adds an Include only mode for field-level adapter scoping in data scopes alongside the existing Exclude mode, with updated labels distinguishing Define asset access by adapter connection from Define field access by adapter connection.

— Names both modes and updated labels but no usage walkthrough.

Axonius Release Notes 9.0.5 (2026-08-20)

12 **Data scope connection selection no longer auto-upgrades**

60

BREAKING

Changes data scope behavior so that selecting all individual connections for an adapter no longer auto-upgrades to adapter-wide selection; the adapter parent checkbox must now be explicitly selected to include current and future connections, meaning new connections won't be automatically covered otherwise.

— States the before/after behavior clearly but no migration steps.

Axonius Release Notes 9.0.5 (2026-08-20)

THINNER COVERAGE BELOW

13 **Impersonated-by field in activity logs** NEW 55

Adds an `Impersonated by` field to HTTP activity logs, recording both the acting user and the impersonated user for all actions taken during an impersonation session.

— Names the field and what it records, no further detail.

Axonius Release Notes 9.0.5 (2026-08-20)

14 **SSL verification enabled by default on new connections**

IMPROVED 55

Changes the default value for SSL certificate verification (`Verify SSL`) from disabled to enabled for all new adapter connections.

— States the exact default change but no rollout guidance.

Axonius Release Notes 9.0.5 (2026-08-20)

15 **IP range operator in Query Wizard** NEW 50

Adds a new `Range` operator for IPv4 field filters in the Query Wizard, enabling From-To IP address range searches.

— Names the operator and its purpose without a worked example.

Axonius Release Notes 9.0.5 (2026-08-20)

16 **Monthly recurrence for historical snapshots** NEW 50

Adds monthly recurrence options for historical snapshot scheduling: first day of month, last day of month, or a specific calendar day.

— Lists the recurrence options but no scheduling walkthrough.

Axonius Release Notes 9.0.5 (2026-08-20)

17 **Unified custom data editing panel** IMPROVED 50

Introduces a unified custom data editing panel on the asset table replacing the separate Create and Edit dialogs, with bulk-edit support for updating shared fields across multiple assets simultaneously.

— Describes the change and bulk-edit capability but no field-level detail.

Axonius Release Notes 9.0.5 (2026-08-20)

18 **Workstation OS exclusion for network routes enrichment** NEW

45

Adds a Workstation OS Types to Exclude setting to Network Routes Enrichment Configurations in Global Settings, letting practitioners exclude specific device operating systems from enrichment.

— Names the setting and location but no further mechanism given.

Axonius Release Notes 9.0.5 (2026-08-20)

└──▷ **ALSO FROM THESE RELEASES**

└──▷ **BREAKING ON UPGRADE**

! Data scope behavior change: selecting all individual connections for an adapter no longer automatically upgrades to an adapter-wide selection; new connections added to the adapter will not be automatically included unless the adapter parent checkbox is explicitly selected.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Ory

Feedback ⓘ 1 RELEASE · 2026-08-20 NOTES ↗

Ory is an open-source identity and access management platform providing authentication, authorization, and user management services.

> Ory refreshed the Console UI with a new design system across self-hosted and Ory Enterprise deployments.

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

01 **Redesigned Console UI** IMPROVED 28

Ory Network's Console UI was refreshed to adopt Ory's new design system, applying to self-hosted and Ory Enterprise deployments.

— Names the change but no specifics on what UI elements changed.

Ory Network, Ory Hydra, Ory Oathkeeper …

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

tailscale

Feedback ⓘ 1 RELEASE · 2026-08-19 BLOG ↗

The easiest, most secure way to use WireGuard and 2FA.

> Tailscale's container image gained a configurable boot timeout for connecting to the coordination server.

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

01 **Configurable boot timeout for container image** NEW 75

The Tailscale container image adds a `TS_BOOT_TIMEOUT` environment variable, accepting a duration value (e.g. `90s` or `3m`) to extend how long the container waits for its initial connection to the coordination server; it defaults to `60s`.

— Names exact env var, format, and default value Tailscale container image v1.102.3 (202…

WAS THIS USEFUL? 👍 👎

◆ Internet Services

Cloudflare

Feedback ⓘ 1 RELEASE · 2026-08-20 BLOG ↗

Cloudflare is a global network platform providing CDN, DDoS protection, DNS, security, and developer services for websites and applications.

> Cloudflare launched Wallets, a programmable payment identity system for account owners and AI agents, alongside nine new models added to the AI catalog, a US-only R2 storage jurisdiction, post-quantum key exchange for Email Security SMTP, and expanded WAF leaked-credential scanning to Authorization headers.

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

01 **R2 `us` jurisdiction for data residency** NEW 90

R2 now supports a `us` jurisdiction guaranteeing data is stored and processed within the United States; access buckets via the jurisdiction-specific S3 endpoint `https://<ACCOUNT_ID>.us.r2.cloudflarestorage.com` or set `jurisdiction = "us"` in a `[[r2_buckets]]` Workers binding.

Create an R2 bucket with US data residency from a Workers configuration to meet explicit US data-locality requirements.

toml

```toml
[[r2_buckets]]
binding = "MY_BUCKET"
bucket_name = "<YOUR_BUCKET_NAME>"
jurisdiction = "us"
```

— Exact endpoint, config key and runnable example given product docs

02 **Cloudflare Wallets for agentic payments** NEW 80

New Cloudflare Wallets product gives Cloudflare accounts and AI agents a stable, human-readable identity and a way to pay for APIs and content using stablecoins. Account Wallets let human owners manage funds and delegate spend to agent-controlled Virtual Wallets, which operate via API keys under a maximum spend cap set by the owner, enabling autonomous agent spending without per-action approval. Wallet handles can be reserved now at `cloudflare.pay` (one per Cloudflare account), publishing a page at `HANDLE.cloudflare.pay` and registering for early access; the system integrates with Agentic Payments so agents can charge for or pay for HTTP content and MCP tools using the x402 protocol.

— Names handle mechanism and protocol but full wallet API not yet live product docs

03 **WAF leaked credentials scans Authorization headers** IMPROVED 80

Cloudflare WAF leaked credentials detection now automatically scans `Authorization: Basic` headers by default; matches populate existing fields such as `cf.waf.credential_check.password_leaked` and trigger the Exposed-Credential-Check managed transform header when configured, so existing custom rules and rate limiting rules apply without modification.

— Names exact fields and header, enabled by default with no setup

WAF - Leaked credentials detection now …

04 **Nine new AI models added to catalog** NEW 75

Workers AI catalog adds `qwen-image-3.0-pro` (Alibaba, text-to-image with up to 6 variants, negative prompts, seed control), `qwen3.7-max` (Alibaba flagship agentic LLM via DashScope), `qwen3.7-plus` (Alibaba, image/video understanding plus coding and GUI automation), `qwen3.8-max` (Alibaba, 2.4T-parameter MoE with native video understanding), Claude Opus 5 (Anthropic, one million token context, no data retention for general access), ByteDance's next-generation video model (text-to-video with up to 30 reference images, 10 reference videos, 10 reference audio clips, first/last-frame image-to-video, video editing/extension, adaptive aspect ratio), `gemini-3.7-flash` (Google, multimodal reasoning for agentic workflows), `ltx-2-5-fast` (Lightricks, fast text/image-to-video with synchronized audio), and `grok-imagine-image-2.0` (xAI, image generation/editing with typography and layout strength).

— Names every model and capability but gives no call syntax product docs

05 **AI Gateway adds `openai/gpt-5.6-sol` promotional pricing** NEW 70

AI Gateway adds support for the `openai/gpt-5.6-sol` model at 50% promotional pricing ($2.50/1M input tokens, $15/1M output tokens, $0.25/1M cache-read tokens)

through September 18, 2026 for non-BYOK users.

— Exact pricing and expiry date but no request example product docs

06 **Post-quantum key exchange for Email Security SMTP** NEW

65

Cloudflare Email Security now negotiates `X25519MLKEM768` post-quantum hybrid key exchange on inbound MX and outbound SMTP delivery connections when the peer supports it, protecting mail traffic against harvest-now, decrypt-later attacks; it is backwards compatible and enabled automatically for all Email Security packages.

— Names exact cipher but change is automatic, nothing to configure product docs

07 **Tunnel origin settings configurable in dashboard** NEW

60

Cloudflare Tunnel now supports configuring origin application parameters — including TLS verification, HTTP Host header, and connection timeouts — directly in the Cloudflare dashboard when editing a published application.

— Names dashboard location and parameters, no API path given product docs

THINNER COVERAGE BELOW

08 **Cloudflare One Client 2026.7.1343.0 graduates to stable**

IMPROVED

55

Cloudflare One Client (Windows, macOS, Linux) version 2026.7.1343.0 graduates to stable with clearer reauthentication notifications with browser redirect, and adaptive HTTP/3-to-HTTP/2 fallback ordering per network to reduce connectivity delays on filtered or legacy networks.

— Exact version number given, no user-facing config product docs

09 **Load balancing analytics filters by pool name** IMPROVED

50

Load balancing analytics pool filter now queries by pool name instead of internal pool ID, fixing filtering for the Requests over time, Pool distribution, Top endpoints, and Latency views and aligning filter behavior with the UI dropdown display.

— Names affected views but only a UI-level fix product docs

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 20, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue