THE CYBER TOOLCHAIN

NO. 040

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 9, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 14 tools

NETWORK SECURITY

vim ? help

◆ Network Analysis & Monitoring

Wireblast

4 RELEASES · 2026-08-02 → 2026-08-03 NOTES ↗

A fast, easy-to-use AF_XDP traffic generator for Linux

> Wireblast shipped as a zero-dependency `AF_XDP` traffic generator hitting 138 Mpps at 100G line rate, then quickly added IPv6 traffic generation, a keep-management receive filter, dashboard refinements, and zero-copy support for AWS ENA NICs.

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

01 Zero-dependency AF_XDP traffic generator binary NEW

88

A single static Go binary implementing `AF_XDP` -based traffic generation — no cgo, no libpcap, no DPDK, no kernel modules. Fully scriptable via `-i` , `--dst-ip` , `--packet-size` , `--pps` , `-d` , `-y` , and `--no-tui` flags for wizard-free packet generation, and delivers measured 100G line-rate performance at all frame sizes, including 138 million packets per second for minimum-size frames from a single process.

Blast 512-byte UDP packets at 1 Mpps for 30 seconds in CI — no wizard, no dashboard, exits with plain-text results.

```
$ sudo wireblast --no-tui -i eth1 --dst-ip 192.0.2.10 --packet-size 512 --pps 1M -d 30s -y
```

— Names exact flags and hard performance numbers. v0.1.0

02 AF_XDP receive mode with flow filters NEW

78

`--mode receive` supports `--rx-mode` filters including `udp-port` (paired with `--rx-port`) for counting arriving packets, and adds a `keep-management` mode allowing broad packet capture on a shared NIC without disrupting the management connection.

Receive all traffic on a shared NIC without dropping the management session, using the new keep-management filter.

```
$ sudo wireblast -i eth1 --mode receive --rx-mode keep-management -d 60s
```

Count arriving packets on a test interface without disturbing the kernel stack — run this in a second window while a sender blasts.

```
$ sudo wireblast -i eth1 --mode receive --rx-mode udp-port --rx-port 9000 -d 60s
```

— Named flags and runnable commands for both filter modes. v0.2.0 v0.1.0

03 **IPv6 traffic generation and multi-flow support** NEW 65

Adds IPv6 support, enabling UDP blasts and multi-flow generation across IPv6 destinations, demonstrated in the `022-ipv6-udp` and `023-ipv6-flows` examples.

Blast UDP traffic to an IPv6 destination to stress-test a dual-stack path or IPv6-only segment.

```
$ sudo wireblast -i eth1 --dst-ip 2001:db8::1 --packet-size 512 --pps 1M -d 30s
```

— Concrete example command against an IPv6 destination. v0.2.0

04 **Interactive TUI wizard and live dashboard** IMPROVED 65

Includes an interactive TUI wizard and live dashboard (Bubble Tea) for guided setup, alongside a `--no-tui` plain-text mode for CI and scripting. The reset action now also clears drop and error counters alongside rate counters, and per-queue drop lines are hidden by default in the live dashboard to reduce noise.

— Describes UI behavior changes but no navigation steps. v0.2.1 v0.1.0

THINNER COVERAGE BELOW

05 **Zero-copy AF_XDP on AWS ENA NICs** NEW 55

Uses page-sized UMEM frames on ENA (AWS Elastic Network Adapter) NICs so that `AF_XDP` zero-copy mode works on ENA-backed instances.

— Mechanism named but no explicit config or command. v0.2.3

06 **Multiple traffic pattern types** NEW 50

Supports UDP, TCP SYN, IMIX (7:4:1 internet mix), raw Ethernet, and PCAP replay (`.pcap` / `.pcapng`) traffic patterns.

Replay a captured trace at a controlled rate to stress-test a device with real-world traffic mix.

```
$ cd examples/015-pcap-replay && IFACE=eth1 DST=192.0.2.10
./run.sh
```

— Lists supported patterns without mechanism detail. v0.1.0

07 **VLAN tagging and multi-flow generation** NEW 50

Supports VLAN-tagged (802.1Q) frame generation, CIDR destination cycling, multi-flow generation (up to thousands of distinct flows), and ECMP/LAG/RSS flow hashing.

— Several named capabilities but no usage example. v0.1.0

08 **Persisted run settings** NEW 50

Remembers last-run settings under `~/.wireblast/` via `internal/prefs` for repeated use.

— Names the path and package but no usage steps. v0.1.0

09 **23 runnable example scripts** NEW 30

Ships 23 runnable example scripts in `examples/` covering benchmarking, IMIX, PCAP replay, VLAN tagging, IPv6, receive mode, and unattended soak tests.

— Bare count and topic list, no specifics on running them. v0.1.0

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Fleet

1 RELEASE · 2026-08-06 NOTES ↗

Open device management

> Fleet 4.90.0 ships in-place configuration profile editing, host naming templates enforced across Apple platforms, multi-package software deployments, custom host vitals, Python packages, Splunk HEC logging, and new Linux platform support (Zorin OS, CachyOS), alongside several breaking changes including removal of the Windows MDM STS endpoint and stricter SCIM access.

└──▷ WHAT SHIPPED · 30 FEATURES most completely described first ? what's the number?

01 Host naming templates across API, GitOps, and enforcement NEW

95

Adds `POST /api/v1/fleet/host_name_template` to set or clear a naming template for a team or `No team` (omitting `fleet_id` or setting it to `0` targets `No team`; an empty template clears enforcement without renaming hosts), `POST /api/v1/fleet/hosts/{id}/name_template/resend` to resend the template to a specific host, and a `name_template` key under `controls` in GitOps (included in `fleetctl generate-gitops` output). Enforcement is now visible for macOS, iOS, and iPadOS under Controls > OS settings > Host names with statuses (Enforcing, Verifying, Verified, Failed) and an `edited_host_name_template` audit activity.

Set a host naming template for all hosts in `No team` so new macOS/iOS/iPadOS enrollments receive a standardized name.

```
$ curl -X POST
https://fleet.example.com/api/v1/fleet/host_name_template \
  -H 'Authorization: Bearer <token>' \
  -H 'Content-Type: application/json' \
  -d '{"name_template": "CORP-$FLEET_VAR_HOST_SERIAL",
"fleet_id": 0}'
```

— Full endpoint set, config key, statuses, and runnable example. fleet-v4.90.0

02 Cross-platform custom disk encryption toggle NEW

85

`FLEET_MDM_ENABLE_CUSTOM_DISK_ENCRYPTION` (`mdm.enable_custom_disk_encryption`) is a new cross-platform alias for `FLEET_MDM_ENABLE_CUSTOM_FILEVAULT`, enabling custom Apple MDM profiles for FileVault and custom Windows configuration profiles for BitLocker from a single setting.

Enable cross-platform custom disk encryption (FileVault + BitLocker) via environment variable on a self-hosted Fleet server.

```
$ FLEET_MDM_ENABLE_CUSTOM_DISK_ENCRYPTION=true fleet serve --config /etc/fleet/config.yaml
```

— Names env var, config key, alias, plus runnable example. `fleet-v4.90.0`

03 **Automatic renewal variable for external CA certificates**

IMPROVED 85

`$FLEET_VAR_CERTIFICATE_RENEWAL_ID` enables automatic renewal for SCEP and ACME certificates issued by external CAs (Okta Conditional Access, Okta Verify, Hydrant ACME) when added to the certificate's Subject OU. It replaces `$FLEET_VAR_SCEP_RENEWAL_ID`, which still works but is deprecated in favor of the new canonical name.

— Names old and new variable, supported CAs, and placement. `fleet-v4.90.0`

04 **Docker-free package building for fleetctl** IMPROVED 85

Removes the `fleetdm/bomutils` Docker dependency from `fleetctl package --type pkg`; Bill of Materials and xar archive are now written in pure Go, removing requirements for Docker, `mkbom`, or `xar`.

— Names command, removed dependencies, and rewrite scope. `fleet-v4.90.0`

05 **New Linux platforms: Zorin OS and CachyOS** NEW 80

Adds Zorin OS as a recognized Linux platform with `platform=zorin`, Linux disk-encryption summary support, `.deb` installs, label platform filter targeting, and CVE matching against Ubuntu LTS OVAL feeds (Zorin 16 → Ubuntu 20.04, 17 → 22.04, 18 → 24.04). Also adds CachyOS (Arch-based Linux) as a recognized Linux platform.

— Names platform values, CVE mapping, and install format for Zorin. `fleet-v4.90.0`

06 **Certificate visibility for Windows and macOS hosts** NEW 78

Adds a certificates list to the host details page for Windows hosts (requires osquery 5.23.1+), showing each certificate's scope (System or User), plus a View certificate modal in Controls > OS settings > Certificates. Also surfaces hardware-bound ACME certificates on macOS host vitals by retrieving them via the MDM `CertificateList` command when an ACME-bearing configuration profile is installed or re-installed.

— Names osquery version requirement, MDM command, and UI path. `fleet-v4.90.0`

07 **Platform filter for policies** NEW 76

Adds an optional `platform` query parameter to `GET /api/v1/fleet/policies` and `GET /api/v1/fleet/fleets/{id}/policies` to filter policies by targeted platform, plus a Targeted platforms column and platform filter dropdown on the Policies page in the UI.

— Names both endpoints and the UI location. fleet-v4.90.0

---

08 **In-place configuration profile editing** NEW 75

`PATCH /api/v1/fleet/configuration_profiles/:profile_uuid` lets admins edit existing configuration profiles in place, covering Apple `.mobileconfig` files, Apple DDM declarations, Windows profiles, and Android profiles.

— Names exact endpoint and platform scope; no worked example. fleet-v4.90.0

---

09 **Custom host vitals fields** NEW 70

Admins can define custom host vitals fields, set values per host manually or via the API, and reference them as `$FLEET_HOST_VITAL_<id>` variables in scripts and configuration profiles.

— Names variable pattern and usage surfaces, no exact API path. fleet-v4.90.0

---

10 **Multiple package versions per software title** NEW 70

Fleet now supports uploading up to 10 custom packages for the same software title on a team, enabling deployment of different versions or architectures (e.g. Arm vs. Intel) to label-scoped hosts, with first-added-wins conflict resolution.

— Explains limit and conflict rule but no exact API/UI path. fleet-v4.90.0

---

11 **Stricter Windows SCEP profile verification** IMPROVED 70

Windows configuration profiles using a Fleet-proxied SCEP certificate now report Verified only after Fleet observes the issued certificate on the host, and report Failed when the SCEP proxy returns an upstream error or the certificate is missing an hour after delivery.

— Explains before/after verification behavior and timing precisely. fleet-v4.90.0

---

12 **Grantable async live query endpoint** IMPROVED 65

The asynchronous live query endpoint `POST /api/v1/fleet/reports/run` is now listed in the API endpoints catalog, making it grantable to API-only users with a restricted allowlist.

— Names endpoint and permission model, no example. fleet-v4.90.0

---

13 **Linux disk encryption key escrow via TPM** NEW 65

Adds support for escrowing disk encryption recovery keys from Linux hosts using TPM-backed full-disk encryption (e.g. Ubuntu 26) via a Fleet-owned snapd recovery key,

silently and without end-user prompting.

– Explains mechanism but no config/API to invoke it. `fleet-v4.90.0`

---

14 **Microsoft Entra conditional access on self-hosted Premium** 65

BREAKING

Enables Microsoft Entra conditional access for self-hosted Fleet Premium instances (previously Fleet Cloud only), gated on the Fleet Premium license tier. As part of this change, the `microsoft_compliance_partner.proxy_api_key` server configuration has been removed since gating now happens via license tier.

– Names removed config key and gating mechanism, no migration steps. `fleet-v4.90.0`

---

15 **Android OS vulnerability reporting** NEW 65

Adds vulnerability (CVE) reporting for Android OS versions on the Software > OS page, including the Android security patch level folded into the OS version string (e.g. `Android 16 (2026-05-01)`).

– Names UI location and version string format, no API. `fleet-v4.90.0`

---

16 **macOS user provisioning and Apple account setup** NEW 65

Adds support for provisioning macOS users during setup and keeping passwords in sync with any OAUTH ROPG-supporting IdP via Fleet Desktop on macOS 26+ hosts, plus a new UI for configuring Apple account provisioning (FPSSO) in the integrations settings.

– Names OS version requirement and IdP protocol, UI path for FPSSO. `fleet-v4.90.0`

---

17 **Removed unused Windows MDM STS endpoint** BREAKING 65

`/api/mdm/microsoft/auth` Windows MDM STS endpoint is removed and now returns a 404. No device ever contacted this endpoint in practice; Windows MDM enrollment via Autopilot, Settings app, and fleetd is unaffected.

– Names exact removed endpoint and unaffected enrollment paths. `fleet-v4.90.0`

---

18 **Python script-only software packages** NEW 60

Adds support for Python (`.py`) script-only software packages as custom packages on macOS and Linux hosts, available via the UI, REST API, and GitOps.

– Names format and surfaces, no specific commands. `fleet-v4.90.0`

19 **Enrollment type selection in Add hosts modal** NEW 60

Adds enrollment profile URL to the macOS tab in the `Add hosts` modal, with enrollment type selection (company-owned or BYOD) for MDM users.

— Names exact UI location and options. fleet-v4.90.0

THINNER COVERAGE BELOW

20 **Disable outbound network blocking for integrations** NEW 55

New `server_bypass_network_blocking` server config option disables all outbound network blocking protections for integration HTTP requests.

— Names config key but no file location or example. fleet-v4.90.0

21 **My device page software tab improvements** IMPROVED 55

Adds installed version and available version columns to the self-service software table on the My device page, and adds an `Applications` / `Full inventory` software filter to the Fleet Desktop My device > Software tab for macOS hosts.

— Names exact UI location and filter options. fleet-v4.90.0

22 **Audit logging for secret variable changes** NEW 50

Adds audit activities when secret variables are created or updated through `PUT /api/latest/fleet/spec/secret_variables`.

— Names endpoint but minimal detail on activity contents. fleet-v4.90.0

23 **Splunk HEC log destination** NEW 50

Adds a native Splunk HEC log destination for osquery status, result, and audit logs.

— Names log types but no config keys given. fleet-v4.90.0

24 **Turn off MDM for offline macOS hosts** IMPROVED 50

Enables the `Turn off MDM` button for offline macOS hosts, queuing the unenroll command for delivery when the device reconnects.

— Names button and queuing behavior, no API. fleet-v4.90.0

25 **DDM user-channel targeting on macOS** NEW 45

Adds support for targeting DDM declarations to the user channel on macOS, and adds the ability to handle DDM assets and additional declaration types.

— Names DDM channel but no config/API path. fleet-v4.90.0

26 **Updated Windows 10 CIS Benchmark policies** IMPROVED 45

Updated CIS Benchmark policies for Windows 10 Enterprise to align with CIS Microsoft Windows 10 Enterprise Benchmark v4.0.0.

— Names exact benchmark version, no list of changed policies. fleet-v4.90.0

27 **Public IP address in host search** IMPROVED 40

Adds public IP address to host search, matching both private and public IPs.

— Thin description, no exact search syntax given. fleet-v4.90.0

28 **Operating systems dashboard card** NEW 30

Adds an Operating systems card to the dashboard when Linux or Android is selected.

— Bare UI addition with minimal context. fleet-v4.90.0

29 **SCIM endpoint restricted to global admins** BREAKING 30

Restricts SCIM endpoint access to global admin users only.

— No endpoint path or migration guidance given. fleet-v4.90.0

30 **Rejects blank enroll secrets** BREAKING 30

Rejects empty and whitespace-only enroll secrets when creating or updating teams.

— Minimal description, no API detail. fleet-v4.90.0

└──▷ **BREAKING ON UPGRADE**

! The `microsoft_compliance_partner.proxy_api_key` server configuration has been removed; Microsoft Entra conditional access is now gated on the Fleet Premium license tier instead.

! The `/api/mdm/microsoft/auth` Windows MDM STS endpoint is removed and now returns a 404 (no device ever contacted this endpoint in practice; Windows MDM enrollment via Autopilot, Settings app, and fleetd is unaffected).

! `$FLEET_VAR_SCEP_RENEWAL_ID` is renamed to `$FLEET_VAR_CERTIFICATE_RENEWAL_ID`; the legacy name still works but `$FLEET_VAR_CERTIFICATE_RENEWAL_ID` is the canonical name going forward.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Axonius ⓘ Axonius Release Notes 9.0.3 (2026-07-22) BLOG ↗

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

Axonius 9.0.3 adds 7 new adapters, a Preferred Last Seen user field, Security Finding count fields by risk level, and dozens of adapter and enforcement enhancements.

└──▷ HOW TO FIND IT

Query devices in the Devices table to surface those with the most critical open security findings, including non-CVE findings, for prioritized remediation.

> 📍 In the Devices table, add the columns Total SF Count: Critical Axonius Risk Level and Total SF Count: High Axonius Risk Level, then filter where Total SF Count: Critical Axonius Risk Level › 0 to identify devices with open critical Security Findings.

Export Jira tickets with team ownership pre-assigned so triage routing happens at ticket creation, not after.

> 📍 In the Enforcement Center, open a Jira Software - Create Ticket action, scroll to the optional Team parameter, enter your team name, and save — newly created tickets will carry that team assignment.

Include a timestamp column in SQL asset exports so downstream pipelines can track when each row was written.

> 📍 In the SQL - Send Assets to Table enforcement action, enable Add Timestamp Column and set Timestamp Column Name to a value such as `axonius_export_ts` before running the action.

- New AI Recommended Action Plans optional field in the Recommended Actions table enables exporting detailed AI-generated action plans to CSV.
- New `Total SF Count: Critical/High/Medium/Low Axonius Risk Level` fields on the Devices table let users query and count non-CVE Security Findings by risk level.
- Checkmarx SAST adapter adds an optional OData API connection method as an alternative integration path, configurable via a new connection setting.
- IBM QRadar adapter adds a new Incidents asset type that fetches QRadar offenses, plus three new advanced settings for time-based and status-based offense filtering; devices are now enriched with related offense information.
- ServiceNow adapter adds a new Custom HTTP Headers connection setting with method and URL pattern filtering support.

+41 more

└──▷ BREAKING ON UPGRADE

- ! Amazon Web Services (AWS) adapter: the `Correlate EKS Containers with their EC2 Instance` advanced setting has been removed; cloud identifiers are now applied automatically.
- ! Qualys Cloud Platform adapter: the Fetch software install paths (CSAM API) advanced setting has been removed; software install paths are now fetched inline from the Inventory API.
- ! Sectigo adapter: the default `Page size` changed from 200 to 100.
- ! OutThink adapter: a new required `Customer ID` connection field has been added; existing OutThink adapter connections must be updated to include it or they will break.
- ! Code42 Incydr adapter has been rebranded to `Mimecast Incydr`; any references to the adapter by its old name will need to be updated.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

DNSFilter ⓘ 1 RELEASE · 2026-08-09 CHANGELOG ↗

DNSFilter is a security tool that filters DNS queries to block malicious domains, ads, and unwanted content at the network level.

> DNSFilter's Query Log gains a one-click Investigate Mode and a policies filter, while dashboards, AppAware and allow/block list management all get incremental upgrades.

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

01 **Investigate Mode in Query Log** NEW 70

A one-click control in the Query Log scopes results to a specific query's timestamp and deployment context, with selectable `±5s`, `±10s`, and `±15s` time windows.

– Names exact time windows but no exact UI path. changelog-20260809-a37458fc

02 **Customizable Dashboards preview** NEW 65

A preview of Customizable Dashboards lets admins build and rearrange widget layouts, apply dashboard-wide filters, save named views with personal defaults, and share views publicly or across an MSP's organizations.

– Describes multiple capabilities but no exact navigation. changelog-20260809-a37458fc

THINNER COVERAGE BELOW

03 **Splashtop support in AppAware** NEW 55

Splashtop has been added to the AppAware application library, enabling policy enforcement and reporting on Splashtop remote desktop traffic.

– Names the specific app and library but little mechanism. changelog-20260809-a37458fc

04 **Conflict validation for Allow/Block lists** IMPROVED 55

Universal and Policy Allow/Block lists now include conflict validation that surfaces which list takes precedence and what will happen when a domain exists in multiple lists.

– Explains behaviour but lacks exact UI location. changelog-20260809-a37458fc

05 **Relocated client admin site-creation toggle** IMPROVED 45

The Client admins can create sites toggle moved from the Whitelabel page to MSP Settings for improved discoverability.

– Small UI relocation, minimal added mechanism. changelog-20260809-a37458fc

06 **Policies filter in Query Log** NEW 35

Admins can now scope Query Log traffic to one or more active policies alongside the existing filters.

— Thin one-line description with no further mechanism. changelog-20260809-a37458fc

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

iDenfy

1 RELEASE · 2026-08-09 CHANGELOG ↗

iDenfy is an identity verification platform that performs KYC/AML checks through document scanning and biometric analysis for compliance.

> iDenfy's Sprint 132 release adds Age Estimation to the dashboard, brings risk assessment data into the company verification API, expands PAYG partner controls, and rounds out digital ID and localization coverage.

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

01 **Age Estimation in dashboard** NEW 50

Age Estimation is now available in the dashboard, covering session creation, filtering, and result details.

– Names dashboard capabilities but no API or config detail changelog-20260809-54b4aab2

02 **KYB risk results and expiration settings** NEW 45

The company verification API now returns risk assessment results in its response payload, and iDenfy adds a configurable KYB company expiration period.

– Describes two KYB additions without endpoint names or config keys

changelog-20260809-54b4aab2

03 **PAYG partner login and billing controls** NEW 40

Adds PAYG social login for Pay-As-You-Go partners, and lets Pay-As-You-Go partners set a dedicated accounting email for invoices and payment receipts.

– Two PAYG features named but no setup steps given changelog-20260809-54b4aab2

04 **New digital ID support for India and Philippines** NEW 30

Adds new digital ID support for India and the Philippines.

– Names countries but no mechanism or usage detail changelog-20260809-54b4aab2

05 **New mobile bottom sheet layout for IDV flows** IMPROVED 25

New mobile bottom sheet layout for IDV flows.

– Bare description of a UI change with no further detail changelog-20260809-54b4aab2

06 **Localization: Spanish business verification and Turkish translations**

IMPROVED

25

Business verification adds Spanish language support, and Turkish translations are improved throughout the product.

— Lists two localization updates without specifics on scope changelog-20260809-54b4aab2

WAS THIS USEFUL? 👍 👎

Auth0 ⓘ 1 RELEASE · 2026-08-09 CHANGELOG ↗

Auth0 is a cloud-based identity and access management platform providing authentication, authorization, and user management solutions for applications.

> Auth0 shipped Session Delegation via Custom Token Exchange, brought Google Workspace Group Sync to General Availability with new admin tooling, and added advanced multi-filter search to Organizations.

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

01 Advanced multi-filter search for Organizations NEW

95

Organizations Search now supports advanced filtering on `Name`, `Display Name`, `ID`, `Metadata` (custom key-value pairs), third-party client access policy (allow or block), and app entitlement status. Up to 5 organization filters can be combined simultaneously using AND/OR logic, with filter state persisted in the URL for sharing or bookmarking.

Filter your tenant's Organizations list to find orgs with a specific metadata tag and third-party client access blocked, then share the view via URL.

> 📍 Navigate to Auth0 Dashboard › Organizations, open the search bar, add a Metadata filter (e.g. `key=tier`, `value=enterprise`) and a Third-party client access filter set to `block`, then copy the URL — the filter pills are persisted in it for sharing or bookmarking.

— Names every filter field, the 5-filter limit, and gives exact navigation steps

changelog-20260809-8ed79864

WAS THIS USEFUL? 👍 👎

Ping Identity

1 RELEASE · 2026-08-09 CHANGELOG ↗

Ping Identity is an enterprise identity and access management platform providing authentication, authorization, and single sign-on solutions.

> Ping Identity's rapid-channel changelog introduces AI agent identities alongside a handful of targeted fixes to SAML metadata import, password hash migration, custom reporting, journey flows, scripting, the promotions API, and WebAuthn credential creation.

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

01 **Skip signature verification on SAML metadata import** NEW

45

Adds the ability to skip signature verification when importing SAML metadata (`OPENAM-26721`).

– Names the ticket and capability but no exact setting or flag.

changelog-20260809-d279054c

02 **Promotions API report metadata ordering** IMPROVED

45

The promotions API now returns report metadata ordered by creation date, most recent first (`FRAAS-33591`).

– Names the API and exact ordering behaviour change. changelog-20260809-d279054c

03 **WebAuthn pubKeyCredParams honored in credential creation**

IMPROVED

45

Advanced Identity Cloud now honors the `pubKeyCredParams` sequence in WebAuthn credential creation requests (`OPENAM-25556`).

– Names the exact field and protocol but no usage example. changelog-20260809-d279054c

04 **PKCS5S2 password hash migration** DEPRECATED

40

Adds support for migrating user accounts from the deprecated PKCS5S2 password hashing scheme to a more secure algorithm (`FRAAS-33086`).

– States the migration path but not the target algorithm or steps.

changelog-20260809-d279054c

05 **Optional parameters in custom reports** IMPROVED

40

Adds the ability to mark parameters in custom reports as optional, giving more flexibility when running reports (`IAM-10610`).

– Names the feature and ticket but no config/UI detail. changelog-20260809-d279054c

06 **Patch Object node v2.0 in journey flows** IMPROVED 40

Adds v2.0 of the Patch Object node in Advanced Identity Cloud journey flows (`OPENAM-26073`).

– Names the specific node and version but no behavioural change described.

changelog-20260809-d279054c

07 **AI agent identities** NEW 25

Introduces AI agent identities to secure AI-driven solutions.

– No detail on scope or how identities are configured. changelog-20260809-d279054c

08 **Send email from next-generation scripts** NEW 25

Adds the ability to send email from next-generation scripts.

– No API, method or scripting hook named. changelog-20260809-d279054c

WAS THIS USEFUL? 👍 👎

ConductorOne

1 RELEASE · 2026-08-08 BLOG ↗

ConductorOne is an identity governance platform that automates access management, provisioning, and compliance workflows across enterprise systems.

> ConductorOne's August 7 release adds a unified Identities & NHI dashboard for tracking human and non-human identities, alongside bulk-revoke for denied access reviews and a quicker way to resume paused MCP servers.

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

01 **Bulk-revoke for denied access reviews** NEW 55

Reviewers can now select multiple denied items from a campaign's Access reviews tab and revoke all at once, rather than revoking one at a time.

– Clear UI action described but no further mechanism detail. August 7, 2026 (2026-08-08)

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Varonis

1 RELEASE · 2026-08-09 CHANGELOG ↗

Varonis is a data security platform that detects and responds to threats targeting sensitive data across cloud and on-premises environments.

> Varonis Atlas introduces Agent Intent-Based Access Control (IBAC), a new capability that monitors AI agents for intent drift, quarantines rogue agents, and audits their behavior across popular coding and AI assistants.

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

01 **Agent IBAC in Varonis Atlas** NEW 66

Varonis Atlas adds Agent Intent-Based Access Control (IBAC) to monitor AI agents for intent drift, validating that an agent's reasoning, tool use, and data access align with its original instructions, and alerting on or blocking deviations. It enables automatic identity quarantine when an agent crosses policy boundaries, blocking all subsequent actions for a defined window, and provides a complete cross-session audit trail for every agent interaction so security teams can confirm agent behavior in real time. It works with agents and AI tools already in use, including Claude Code, Cursor, GitHub Copilot, and Microsoft Copilot Studio, with no replacement of existing tooling required.



— Explains mechanism and named integrations but no config or command to enable it.

changelog-20260809-1615cb69

WAS THIS USEFUL? 👍 👎

◆ Integrated & IT Risk Management

CISO Assistant

1 RELEASE · 2026-08-08 NOTES ↗

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 150+ 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 v3.21.0 introduces MITRE ATLAS-based threat modeling, a drag-and-drop visual workflow engine, focus-mode scoped permissions, and service account management, alongside smaller upgrades to frameworks, asset classes, findings-assessments and document tracking.

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

01 **TTP support and threat modeling with MITRE ATLAS** NEW

35

Introduces TTP (tactics, techniques, procedures) support and threat modeling capabilities, including the MITRE ATLAS framework.

— Names MITRE ATLAS but no mechanism or UI path given. v3.21.0

02 **Visual workflow engine with drag-and-drop builder** NEW

30

New visual workflow engine with a drag-and-drop builder for automating security processes.

— Describes capability but not how to configure it. v3.21.0

03 **Focus-mode with scoped permissions** NEW

30

Adds focus-mode with scoped permissions and enhanced user context controls.

— No detail on how scoping or context controls work. v3.21.0

04 **Cwb NIS2 control framework and framework updates** IMPROVED

30

Adds the Cwb (NIS2) Control Framework plus additions and updates to existing framework tools.

— Names new framework but not what other updates entail. v3.21.0

05 **Plumber CI/CD hardening checks library** NEW

30

Adds a plumber CI/CD hardening checks library.

— Named library but no usage instructions given. v3.21.0

06 **Customizable asset classes with hierarchical tree view** IMPROVED

30

Asset classes are now fully customizable and can render as a full hierarchical tree.

— Explains change but not configuration steps. v3.21.0

07 **Progress percentage calculation for documents** NEW

30

Adds progress percentage calculation based on status to documents.

— States mechanism (status-based) but no formula or UI location. v3.21.0

08 **Service account management for programmatic access** NEW

25

Adds service account management (pro) for programmatic access.

— Bare feature name, no config or endpoint detail. v3.21.0

09 **Status tracking for findings-assessments** NEW

25

Adds status tracking to findings-assessments.

— Bare mention, no status values or workflow detail. v3.21.0

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Cline

4 RELEASES · 2026-08-09 NOTES ↗ CODE ↗

Autonomous coding agent as an SDK, IDE extension, or CLI assistant.

> Cline shipped OAuth authorization support for remote MCP servers, more resilient session and turn handling across aborts and network interruptions, richer scheduled run reporting, and a new `cline mcp uninstall` CLI subcommand across its desktop, IDE, CLI and SDK surfaces this window.

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

01 Session and turn resilience across aborts and interruptions

IMPROVED 72

Prompts queued during a turn now survive interruption — preserved across aborts, drained after a turn aborts itself, with edits made inside the abort window applied rather than lost, and failures reported as `run.failed` instead of completing silently. Session context stays durable across aborts and hub restarts, so an interrupted session resumes with its prior state, and mid-stream network interruptions occurring before any model output are retried instead of failing the turn.

— Names the `run.failed` signal and durability scope, no user command desktop-v0.0.11 cli-v3.0.52 sdk/sdk/v0.0.72

02 Provider connectivity fixes for LiteLLM and Vertex ADC IMPROVED

62

LiteLLM requests now route through Chat Completions instead of the Responses API, enabling calls against LiteLLM proxies, and Vertex ADC token refreshes now use the configured fetch so they work behind proxies and custom transports.

— Names the exact APIs swapped but no user-facing flag desktop-v0.0.11 cli-v3.0.52 sdk/sdk/v0.0.72

THINNER COVERAGE BELOW

03 Scheduled run reports and provider settings reuse IMPROVED

57

Scheduled run reports now carry execution context including readable headers, schedule metadata, durations, and lifecycle error details, and schedules now reuse saved provider settings instead of requiring separate provider configuration.

— Lists report fields and reuse behavior but no API/flag desktop-v0.0.11 v4.1.7 cli-v3.0.52 sdk/sdk/v0.0.72

04 **Hung MCP server handling during session creation** IMPROVED

55

A hung MCP server no longer blocks session creation, and stdio servers that were never configured now get a 30-second initialize budget instead of blocking indefinitely.

— Gives the exact 30-second timeout but no user-facing control `desktop-v0.0.11` `cli-v3.0.52` `sdk/sdk/v0.0.72`

05 **Checkpoint tracking for untracked files and mid-session git init**

IMPROVED

53

Checkpoints are now picked up when git is initialized mid-session, and checkpoint diffs include files that were untracked at the time the snapshot was taken.

— Describes the before/after behavior but no config surface `desktop-v0.0.11` `cli-v3.0.52` `sdk/sdk/v0.0.72`

06 **Centralized plugin settings management** IMPROVED

45

Plugin settings and contributions are now managed centrally with host-aware snapshots and atomic plugin toggles, and empty install directories are no longer listed as installed.

— Describes mechanism but no config key or command exposed `desktop-v0.0.11` `v4.1.7` `sdk/sdk/v0.0.72`

07 **Readable MCP tool results in TUI** IMPROVED

40

MCP tool results now render as readable text in the TUI instead of escaped JSON, and binary payloads survive being expanded.

— Describes rendering change but no command to invoke `cli-v3.0.52`

08 **Lazy loading for Settings, Sessions, Onboarding, Diff views**

IMPROVED

35

Settings, Sessions, Onboarding, and Diff views now load lazily for improved startup performance.

— Names the four views but no measured performance gain `desktop-v0.0.11`

09 **Clipboard image paste in composer** NEW

33

Supports pasting images directly from the clipboard into the composer.

— Clear UI action but no further mechanism given `desktop-v0.0.11`

10 **Folder picker failure handling** IMPROVED

32

The folder picker now reports failures and offers a manual path entry as a fallback.

— Names the fallback but no further detail `desktop-v0.0.11`

11 **Copy button on turn-final responses** NEW 23

Adds a copy button to turn-final response rows.

— Bare UI addition with no further detail `v4.1.7`

12 **Folder-aware welcome suggestions** IMPROVED 23

Welcome suggestions now adapt to what is actually in the opened folder instead of assuming a code project.

— Describes behavior change with no mechanism `desktop-v0.0.11`

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ Agentic Infrastructure

emisar

1 RELEASE · 2026-08-08 NOTES ↗

An MCP that lets AI tools securely connect to your infrastructure, write IaaS code, debug issues, and assist during incidents - without risking production stability. Built for security teams to approve and infrastructure teams to experience like magic.

> Emisar v0.38.0 adds a safety check for ineffective policy override globs and fixes a bug where terminating a member's sessions failed to disconnect the live console session.

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

01 **Invalid-glob warning for policy overrides** NEW 67

Emisar now shows a real-time advisory warning when a policy override glob cannot match any action ID (e.g. regex-style patterns like `cassandra\.drop_*`), flagging deny rules that look protective but cover nothing. The warning is non-blocking, so rules targeting not-yet-installed packs are still allowed.

— Explains mechanism and example pattern but no UI path given. v0.38.0

THINNER COVERAGE BELOW

02 **Session termination disconnects live console session** IMPROVED 50

Ending a member's sessions now disconnects the live console session itself, not only the cookie behind it, so administrator-initiated session termination during an incident takes effect immediately.

— Clear before/after but no command or endpoint named. v0.38.0

WAS THIS USEFUL? 👍 👎

◆ Local LLM Runtimes

vMLX ⓘ 1 RELEASE · 2026-08-08 NOTES ↗

vMLX - JANGTQ Uber Compressed MLX Models - L2 Disk Cache (survives restart) + L1 Paged (super fast ttft) + Hybrid SSM Scheduler + Cont Batching + etc!

> vMLX 1.6.25 focuses on DeepSeek V4 prefill speed and long-context robustness: a new indexed-attention kernel delivers a 29–58% prefill throughput gain, KV cache rewind cuts retry time-to-first-token to under 3 seconds, KV cache reuse and quantization reduce redundant work and RAM use, and oversized requests now get a clean 413 instead of a Metal OOM crash.

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

01 Indexed-attention prefill kernel for DeepSeek V4 IMPROVED

80

A new indexed-attention prefill kernel, enabled by default, lifts DeepSeek V4 Flash prompt processing from 347 to ~449 tokens/s at 15k context (+29%) and from 199 to ~316 tokens/s at 40k context (+58%), while sustaining 33+ tokens/s decode at both lengths.

— Concrete before/after throughput numbers but automatic, no user-facing switch v1.6.25

02 Memory ceiling reporting and clean 413 on OOM IMPROVED

70

The engine now advertises the true hardware memory ceiling at startup, adaptively shrinks prefill chunks under Metal memory pressure, and returns a clean `413` error on over-ceiling requests instead of crashing with a Metal OOM; the flat request timeout that previously killed healthy very-long prefills has also been removed.

— Names concrete HTTP status and behavior a client can handle v1.6.25

03 KV cache rewind on abort/retry NEW

65

On abort or retry, the engine rewinds the live KV cache to the shared prefix instead of re-prefilling from scratch, dropping retry time-to-first-token at 15k context from 46s to 2.3s.

— Clear mechanism and numbers, but behavior is automatic v1.6.25

THINNER COVERAGE BELOW

04 KV pool quantization caps cache RAM IMPROVED

45

KV pool quantization keeps cache RAM under 8 GB even near the model's maximum context.

— Names a concrete RAM ceiling but no mechanism detail v1.6.25

05 **KV cache reuse in two-pass answer path** IMPROVED 40

The two-pass answer path now reuses the first pass's KV cache, eliminating a full prompt re-prefill on the second pass.

— States what changed but no numbers or mechanism detail v1.6.25

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

Daytona

1 RELEASE · SEEN 2026-08-09 NOTES ↗

Daytona is a development environment platform that enables standardized, reproducible coding spaces for teams and AI agents.

> Daytona 0.200.0 focuses on security hardening, enforcing TLS verification across client libraries, locking down CLI config file permissions, and giving the Go SDK a configurable HTTP timeout for long-running executions.

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

01 **CLI config file restricted to owner permissions** IMPROVED

45

The CLI config file is now created with `0600` permissions, restricting access to the owner only.

– Exact permission mode named, but no file path or migration note snapshot-20260809

02 **Configurable HTTP timeout in Go SDK** NEW

40

The Go SDK now supports a configurable HTTP timeout, allowing long-running executions to be handled reliably instead of timing out on default settings.

– Names the SDK and capability but no config key or value snapshot-20260809

03 **TLS verification enforcement in client libraries** BREAKING

35

Daytona 0.200.0 enforces TLS verification in the Ruby Socket.IO client and across the client security layer more broadly, tightening how clients validate connections.

– Security change named but mechanism and impact scope unclear snapshot-20260809

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 9, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe