THE CYBER TOOLCHAIN

NO. 064

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 4, 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 269 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 39 tools

▾ // THE BRIEF

HIDE SAME ISSUE, SAME PROMPT, TWO WRITERS: GPT-5.5 Opus 5

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 today: Endor Labs can stop bad packages before install, ZeroPath re-triages new CVEs against existing

vim ? help

inventory within minutes, and DigiCert CertCentral keeps domains issuance-ready without manual validation work.

> PROTECT
>
> **Block risky dependencies before they land on a developer machine or builder**
>
> Package Firewall moves dependency control to install time, so malicious, vulnerable, or non-compliant packages can be denied before they reach disk. That closes the gap where a scanner finds the problem only after the package is already in the workspace or build path.
>
> Endor Labs

> PROTECT
>
> **Re-triage new CVEs against the software you already inventoried**
>
> ZeroPath now continuously checks new advisories against existing SCA inventory and exports reachability-aware SBOM, VEX, and AI-BOM data. Teams get faster vulnerability prioritization without re-running manual analysis just to learn whether a fresh CVE matters to code they actually ship.
>
> ZeroPath

> GOVERN
>
> **Keep release evidence tied to the controls auditors ask for**
>
> AppTrust added automated release-evidence traceability and built-in NIST SSDF and EU CRA frameworks. That turns provenance and compliance evidence into a maintained release artifact instead of a spreadsheet or hand-written policy layer assembled after the fact.
>
> JFrog

> PROTECT
>
> **Keep domains ready for certificate issuance without repeating validation work**
>
> Continuous Validation automates DNS-based domain control validation so domains can stay issuance-ready. That reduces the manual DCV chase that often appears only when a certificate needs to be issued or renewed quickly.
>
> DigiCert CertCentral

Does **GPT-5.5** read better? 👍 👎

◆ AI-Powered Offensive Security

T3MP3ST

Feedback ⓘ changes since 2026-09-03 CODE ↗

autonomous red teaming platform; multi-agent offensive-security meta-harness

T3MP3ST gains CISA KEV/EPSS feed ingestion, CVE correlation API, alert delivery, honeytoken lifecycle, CTF labs, and more.

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-09-03 https://github.com/elder-plinius/T3MP3ST.git
# already have the repo? check out this version:
$ git checkout commits-2026-09-03
```

└──▷ TRY IT

Route honeytoken trigger alerts to Slack by setting the webhook URL before running T3MP3ST.

```
$ export SLACK_WEBHOOK_URL='https://hooks.slack.com/services/T00/B00/xxxx'
export DISCORD_WEBHOOK_URL=''
export SIEM_WEBHOOK_URL=''
```

Adds provenance-safe threat feed ingestion for `cisa-kev` and `first-epss` sources (via `CISA_KEV_URL` and `FIRST_EPSS_URL`), with typed `KevRecord` and `EpssRecord` normalization, bounded HTTP reads, deterministic deduplication, independent per-source failure isolation, and stale-cache fallback via a `FeedCache` interface.

Adds a CVE correlation API that maps technology names to KEV/EPSS candidates using caller-supplied `ThreatFeedSnapshot` data, with provenance preserved on every result and all matches classified as unverified candidates — no network access at correlation time.

Adds secure alert delivery (`src/integrations/alerts.ts`) supporting `'slack'`, `'discord'`, and `'siem'` providers, configured via `SLACK_WEBHOOK_URL`, `DISCORD_WEBHOOK_URL`, and `SIEM_WEBHOOK_URL` environment variables, with `AlertDestinationSpec` controls for `proxyPolicy`, `maxAttempts`, `rateLimitMs`, and `maxPayloadBytes`.

Adds a scoped honeytoken lifecycle with a `HoneytokenAlertSink` / `HoneytokenTrigger` interface wired into the alert delivery layer.

Adds opt-in bounded context compression (`src/llm/context-compression.ts`) with explicit `ContextKind` and `ContextTrust` classification, token budgeting via `CompressionOptions` (`tokenBudget`, `summaryTokenBudget`), and full `ContextAccounting` reporting of retained, summarized, dropped, and overflowed items — system policy, authorization, evidence, citations, and unresolved errors are never summarized or dropped.

+6 more

WAS THIS USEFUL? 👍 👎

Keygraph shannon

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗

RANK

Shannon is an AI pentester for web applications and APIs. It analyzes your source code, identifies attack vectors, and executes real exploits to prove vulnerabilities before they reach production.

> Shannon v3.1.0 adds support for configuring a custom base URL per provider for the OpenAI Responses API, letting teams point at self-hosted models or gateways.

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

01 **Custom base URL for OpenAI Responses API** NEW 65

Adds per-provider custom base URL configuration for the OpenAI Responses API, enabling use of self-hosted models, gateways (e.g. OpenRouter, LiteLLM), or any other compatible endpoint.

— Names the API and example gateways but no exact config key or flag. v3.1.0

WAS THIS USEFUL? 👍 👎

◆ Post-Exploitation

InGuardians peirates

Feedback ⓘ 1 RELEASE · 2026-09-04

NOTES ↗ RANK

Peirates - Kubernetes Penetration Testing tool

> Peirates v1.1.31 adds a new container escape technique for privileged containers that share the host PID namespace.

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

01 **Escape privileged containers via host PID namespace** NEW

50

A new menu item lets operators break out of privileged containers that share the host's PID namespace, adding a new container escape technique usable from within a Kubernetes environment.

— Names the technique and menu addition but no exact steps. v1.1.31

WAS THIS USEFUL? 👍 👎

◆ Exploitation & C2

Bishop Fox sliver

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗

RANK

Adversary Emulation Framework

> Sliver v1.7.7 focuses on tunnel reliability, adding OPFOR CNA BOF scripting support and hardening portfwd/SOCKS5 connections alongside a reworked reverse port forwarding lifecycle.

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

01 **Portfwd and SOCKS5 tunnel hardening** IMPROVED 50

Hardens `portfwd` and SOCKS5 tunnels for improved reliability and stability, and reworks the reverse port forwarding lifecycle with end-to-end coverage improvements.

— Names affected surfaces but no mechanism detail v1.7.7

02 **OPFOR CNA BOF scripting** NEW 15

Adds OPFOR CNA BOF scripting support, as noted in the release summary.

— Only mentioned in title/summary, no further detail v1.7.7

03 **Windows shell handling improvements** IMPROVED 15

Improves Windows shell handling.

— Bare statement with no mechanism or scope v1.7.7

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

LavaMoat

Feedback ⓘ 2 RELEASES · 2026-09-03 NOTES ↗ RANK

tools for sandboxing your dependency graph

> LavaMoat shipped policy-regeneration and Web Worker fixes for its webpack plugin, plus a JSON output mode and wildcard script matching in harden.

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

01 **JSON output for harden check** NEW 75

Adds a `--json` option to the `harden check` command for machine-readable output, useful for feeding results into a CI pipeline or SIEM.

Output harden check results as JSON for ingestion into a CI pipeline or SIEM.

```
$ harden check --json
```

– runnable command with example given harden-v0.7.0

THINNER COVERAGE BELOW

02 **Policy overwrite flag in webpack plugin** NEW 55

Adds an opt-in flag to the LavaMoat webpack plugin that lets it overwrite `policy.json` with overrides, enabling automated policy regeneration workflows.

– names config file but not exact flag webpack-v2.3.0

03 **importScripts capture under scuttling** IMPROVED 55

The webpack plugin now captures the `importScripts` reference for use in the webpack runtime even when scuttling is enabled, unblocking Web Worker builds that rely on `importScripts`.

– explains fix but no user-facing action needed webpack-v2.3.0

04 **Wildcard prefix matching in scriptsConfig** NEW 55

Adds wildcard prefix matching for `scriptsConfig` entries in the harden runner, allowing glob-style script name patterns.

– config key named but no usage example harden-v0.7.0

WAS THIS USEFUL? 👍 👎

Endor Labs

Feedback ⓘ 2 RELEASES · 2026-09-03 BLOG ↗ RANK

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

> Endor Labs shipped Package Firewall, a new install-time enforcement layer that blocks malicious, vulnerable, and non-compliant packages before they reach disk, and extended its Bazel `rules_apple` software composition analysis to watchOS, tvOS, and visionOS targets.

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

01 Package Firewall for blocking risky packages at install NEW

86

Package Firewall intercepts every package install request and returns a `403` for flagged packages so they never touch disk, while clean packages are transparently redirected to the upstream registry. It integrates with private artifact managers (e.g. JFrog Artifactory) by pointing a remote repository at the Package Firewall URL with no developer-machine changes, or runs in Endpoint Mode where configuration is pushed to developer machines via MDM and to CI runners via a config snippet. It enforces configurable cooldown periods that block newly published package versions for a set window regardless of requester, and plugs into the Endor Labs policy engine to block packages with known CVEs or license non-compliance in addition to malware. Every install event (package name, version, time, reason) is logged and visible in the Endor Labs UI and via the API, powered by a real-time malware feed that uses multi-pass LLM, static, and behavioral analysis to classify newly uploaded npm, PyPI, and Go packages within minutes of upload.

— Rich mechanism and named surfaces but no CLI/API syntax given

Introducing Package Firewall | Blog | E… launch-20260903-d7431612

THINNER COVERAGE BELOW

02 Bazel rules_apple SCA extended to watchOS, tvOS, visionOS

IMPROVED

55

Endor Labs now supports dependency resolution for `watchos_application`, `tvos_application`, `visionos_application`, and their related framework and test rules in Bazel `rules_apple` workspaces, extending existing iOS and macOS software composition analysis coverage.

— Names exact Bazel rules but gives no usage steps product docs

WAS THIS USEFUL?  

GitHub

Feedback ⓘ 4 RELEASES · 2026-09-03 BLOG ↗ RANK

Join the world's most widely adopted, AI-powered developer platform where millions of developers, businesses, and the largest open source community build software that advances humanity.

> GitHub's biggest shifts this window were security-focused: npm trusted publishing gained multiple OIDC configurations with malware-scan gating, GitHub Actions picked up a runner deprecation API and a least-privilege Dependabot permission, and CodeQL 2.26.4 sharpened Actions pinning checks alongside new taint-flow and Go 1.27 coverage. Gemini 3.8 Flash also became selectable across Copilot surfaces.

└──▷ **WHAT SHIPPED · 11 FEATURES** most completely described first ? what's the number?

01 **Runner deprecation API for GitHub Actions** NEW 90

Adds `GET /actions/runners/deprecations/{version}`, available at repository, organization, and enterprise level, returning `runner_version`, `runtime_deprecates_at`, and `registration_deprecates_at` so teams can plan runner upgrades before support ends.

Check when a specific runner version loses runtime and registration support, so you can schedule upgrades before deprecation.

```
$ curl -H "Authorization: Bearer <token>" \
  -H "Accept: application/vnd.github+json" \
  https://api.github.com/actions/runners/deprecations/2.315.0
```

— Exact endpoint, fields, and a runnable curl example

GitHub Actions: Early September 2026 up…

02 **Job context properties for reusable workflows** NEW 85

Adds four new `job` context properties for reusable workflows — `job.workflow_ref`, `job.workflow_sha`, `job.workflow_repository`, and `job.workflow_file_path` — letting a reusable workflow determine its own source identity at runtime; not available on GitHub Enterprise Server.

Surface the exact source file and commit of a reusable workflow at runtime for audit logging or conditional logic.

```yaml
jobs:
  called-job:
    runs-on: ubuntu-latest
    steps:
      - name: Print reusable workflow identity
        run: |
          echo "Workflow ref: ${{ job.workflow_ref }}"
          echo "Workflow SHA: ${{ job.workflow_sha }}"
          echo "Repository:   ${{ job.workflow_repository }}"
          echo "File path:    ${{ job.workflow_file_path }}"
```

— Four named properties with a runnable YAML example

GitHub Actions: Early September 2026 up…

---

03 **vulnerability-alerts permission for GITHUB_TOKEN** NEW

80

Adds a `vulnerability-alerts` permission for `GITHUB_TOKEN` supporting `read` and `none` values, enabling least-privilege read-only access to Dependabot alerts without granting broader repository scopes.

Grant a workflow read-only access to Dependabot alerts using least-privilege scoping instead of broad repository permissions.

```yaml
permissions:
  vulnerability-alerts: read

jobs:
  audit-alerts:
    runs-on: ubuntu-latest
    steps:
      - name: List Dependabot alerts
        run: gh api repos/${{ github.repository
}}/dependabot/alerts
```

— Named permission and values with a working workflow snippet

GitHub Actions: Early September 2026 up…

---

04 **GitHub Actions security detection improvements in CodeQL**

IMPROVED

75

The `actions/unpinned-tag` query now detects mutable references to reusable workflows, expanding pinning enforcement beyond actions to workflow calls.

`EnvironmentCheck` can now be specified through a models-as-data model, allowing custom environment sanitizer definitions without modifying queries. Actor-field checks on fields like `github.event.pull_request.user.login` now only count as protection for events that actually populate that field, reducing false negatives in `ControlCheck` `-based` queries — though this may cause `ControlCheck` `-based` queries to surface more alerts since environments are no longer treated as a sufficient sanitizer.

— Names three query mechanisms and their before/after behavior

CodeQL 2.26.4 improves GitHub actions s…

---

05 **Multiple trusted publishing configurations for npm** IMPROVED

65

npm packages can now have multiple trusted publishing (OIDC) configurations, each with its own repository, workflow, and environment criteria — a publish or stage succeeds if the incoming OIDC token matches any one configuration. Direct publishing is now opt-in per configuration (staging-only is the default, and every configuration can stage without extra setup), the staged publishing queue's approval button disables during malware scanning and re-enables once the scan completes (refreshing status every minute), and the versions tab on npmjs.com now shows a per-version staged history noting whether each version was approved, rejected, or remains staged.

— Describes mechanism and UI behavior but no config keys or exact steps

Multiple trusted publishing configurati…

---

06 **Expanded taint-flow and syntax coverage across languages**

IMPROVED

65

CodeQL adds taint flow through `list.extend` and `list.insert` in Python (matching existing `list.append` coverage), taint propagation through String.valueOf(Object) when the argument is a `CharSequence` (e.g., `String` or `StringBuilder`) in Java/Kotlin, and support for regular expressions using the `d` flag and the React Native Worklets `'worklet'` directive in JavaScript/TypeScript.

— Names every method and syntax feature but is purely informational

CodeQL 2.26.4 improves GitHub actions s…

---

07 **Gemini 3.8 Flash in Copilot** NEW

60

Gemini 3.8 Flash is now selectable in the Copilot model picker across Visual Studio Code, Visual Studio, Copilot CLI, GitHub Copilot cloud agent, GitHub Copilot app, JetBrains IDEs, Xcode, and Eclipse. Enterprise and Business admins can manage access via the model policy in Copilot settings, including a default model enablement toggle that auto-enables new models unless explicitly disabled.

Enable or restrict Gemini 3.8 Flash for your organization before the gradual rollout reaches all users.

📍 In GitHub Copilot settings, go to Settings › Copilot › Model policy › Default model enablement and explicitly enable or disable Gemini 3.8 Flash for your Enterprise or Business plan.

— Names surfaces and admin toggle but only a UI navigation path

Gemini 3.8 Flash is now available in Gi…

THINNER COVERAGE BELOW

08 **SQL injection sink models for Spring R2DBC** NEW 55

Adds SQL injection sink models for Spring R2DBC `DatabaseClient` and the R2DBC SPI, covering reactive database access patterns in Java/Kotlin.

— Names the exact API surfaces but no usage example

CodeQL 2.26.4 improves GitHub actions s…

09 **Antiforgery token recognition in CodeQL** IMPROVED 50

The `cs/web/missing-token-validation` query now recognizes enabled ASP.NET Core `RequireAntiforgeryToken` attributes when antiforgery middleware is used, reducing false positives for protected endpoints.

— Names the query and attribute but no runnable steps

CodeQL 2.26.4 improves GitHub actions s…

10 **Rust data flow alert location fix** BREAKING 45

Rust data flow query alert locations now reflect actual source and sink nodes; some alerts will change location, appearing as new alerts while previous alerts at the old location close.

— Explains before/after alert behavior but no migration steps

CodeQL 2.26.4 improves GitHub actions s…

11 **Go 1.27 language support in CodeQL** NEW 30

Adds Go 1.27 language support to CodeQL.

— Bare one-line addition with no further detail CodeQL 2.26.4 improves GitHub actions s…

└──▷ **BREAKING ON UPGRADE**

! Rust data flow query alert locations now reflect actual source and sink nodes — some alerts will change location, appearing as new alerts while previous alerts close.

! GitHub Actions `ControlCheck` `-based` queries may produce more alerts because actor fields from event payloads are no longer treated as protection for events that do not populate them, and environments are no longer a sufficient sanitizer.

WAS THIS USEFUL? 👍 👎

Cloudsmith

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

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

> Cloudsmith extended its cooldown policy protection to Cargo packages, letting teams delay consumption of newly published crates.

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

01 **Cooldown policies for Cargo packages** NEW 50

Cooldown policies now extend to Cargo packages, blocking newly published versions from being consumed until a configured delay period has passed, providing supply chain protection for Rust dependencies.

— Explains mechanism and scope but no config details or limits.

Cooldown policies now support Cargo (20…

WAS THIS USEFUL? 👍 👎

JFrog

Feedback ⓘ 2 RELEASES · 2026-09-02 BLOG ↗ RANK

JFrog software supply chain solutions provide an end-to-end pipeline to control your binaries from build to production. Power your software updates to the edge.

> JFrog AppTrust gained automated release-evidence traceability and out-of-the-box compliance frameworks, letting teams prove SDLC provenance and enforce NIST SSDF and EU CRA controls without hand-writing policy code.

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

01 **NIST SSDF and EU CRA compliance frameworks** NEW 73

AppTrust adds out-of-the-box compliance frameworks, starting with NIST SSDF and EU CRA, with controls pre-mapped to Policy-as-Code rules so teams can enable enforcement without writing Rego manually. Framework configuration is separated from rollout control: AppSec owns which controls and rules are active, while development managers configure which applications fall under the framework, whether rules run as warnings or hard failures, and how long before a warning converts to a blocked package.

— Names frameworks and Policy-as-Code mechanism; points to Compliance Catalog UI

launch-20260902-7632a07c

02 **Prompt to Release Traceability in AppTrust** NEW 66

JFrog AppTrust automatically collects and signs commits, pull requests, Jira ticket transition histories, and approver chains for every release before any promotion gate runs. It automatically flags self-approval violations by checking whether the PR approver is the same person as the committer, a check most compliance frameworks require but few teams automate. Upcoming JFrog Agent Plugins will extend this to capture AI agent session evidence — prompts, code produced, MCPs, skills, and agentic assets used — as signed evidence stored in Artifactory, and this SDLC traceability is described as connecting AI agent intent sessions alongside Git commits, pull requests, and Jira tickets to the artifacts that ship.

— Clear mechanism and named checks, but no config key or command given

launch-20260902-e709d19a launch-20260902-7632a07c

WAS THIS USEFUL? 👍 👎

StepSecurity

Feedback ⓘ 3 RELEASES · 2026-09-02 BLOG ↗ RANK

StepSecurity is a security hardening platform that reduces attack surface and prevents supply chain attacks in GitHub Actions workflows.

> StepSecurity's biggest window addition is continuous PAT governance across GitHub and Azure DevOps, alongside deny-list egress policies for Harden-Runner and native support for AWS CodeBuild-hosted GitHub Actions runners.

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

01 Deny-list egress policies across Harden-Runner surfaces NEW

95

Adds a `denied-endpoints` input to `step-security/harden-runner` (v2.21.0) to block named domains, wildcard domains (e.g. `*.example.org`), or IP addresses while leaving all other destinations reachable under `egress-policy: block`. The same deny-list capability ships as `denied_endpoints` on the Self-Hosted VM Harden Runner (v1.9.0), and as a Policy Store option attached at organization or cluster scope via ARC Harden Runner v2.19.0+, enforcing CI egress restrictions across all repositories without per-workflow-file edits.

Block direct npm and PyPI registry access org-wide to enforce routing through a package proxy, while leaving all other outbound traffic unrestricted.

yaml

```yaml
- uses: step-security/harden-runner@v2.21.0
  with:
    egress-policy: block
    denied-endpoints: |
      registry.npmjs.org
      pypi.org
      files.pythonhosted.org
```

— Names exact inputs and versions with a runnable config example launch-20260902-57163262

02 Runtime security for AWS CodeBuild-hosted GitHub Actions runners

NEW

95

`step-security/harden-runner@v2.20.1` adds support for GitHub Actions jobs running on AWS CodeBuild EC2 compute, monitoring outbound network calls, file writes, and process execution; v2.21.0 extends this to Linux containers on EC2, including custom images from Amazon ECR and external Docker registries. Requires the

CodeBuild project set to `Compute: EC2`, `Host kernel: kernel-6` (Amazon Linux 2023), and `Privileged: Enabled` in the project's `Additional configuration` panel. It surfaces memory-read detections (the technique behind CVE-2025-8217) as a runtime alert with an attached triage runbook, and unifies CodeBuild-hosted, GitHub-hosted, ARC, and self-hosted runner fleets under a single dashboard, Policy Store, and detection baseline.

Secure a CodeBuild-hosted GitHub Actions job to monitor all outbound network calls and process executions from inside your AWS VPC.

```yaml
jobs:
  build:
    runs-on: codebuild-my-project-${{ github.run_id }}-${{
github.run_attempt }}
    steps:
      - uses: step-security/harden-runner@v2.21.0
        with:
          egress-policy: audit
      - uses: actions/checkout@v4
```

— Exact versions, config keys, and a runnable workflow snippet `launch-20260902-ce9382ed`

03 **Token Controls policy engine for PAT governance** NEW

85

Token Controls evaluate the entire PAT inventory hourly across both GitHub and Azure DevOps organizations, surfacing breaching tokens as findings on the All Controls dashboard with evidence, impact, and a per-token revoke action. Organizations can set configurable max-age and idle-window thresholds, with separate limits for fine-grained versus classic GitHub tokens and a stricter limit for high-privilege Azure DevOps tokens, plus pre-expiry reminder notifications to token owners at configurable bands (30, 7, and 1 days by default) on both platforms. Scope risk classification flags Azure DevOps tokens against the 35 Microsoft-rated high-privilege scopes with colour-coded scope chips, while on GitHub it flags coarse classic scopes (`repo` , `admin:org` , `workflow`) and fine-grained tokens combining all-repository access with write permissions. Per-control notification events fire once when a token first breaches policy rather than on every scan, and each control's notifications are selectable independently.

Triage PATs currently breaching your token policy — including over-privileged classic GitHub tokens with `repo` or `admin:org` scope — and revoke offenders directly from the dashboard.

📍 In the StepSecurity console, go to All Controls dashboard, filter by Token Controls, review each finding's evidence and impact, then click `Revoke` on any

token that breaches the policy.

— Names exact scopes, thresholds, and notification bands with a revoke workflow

PAT Governance for GitHub and Azure Dev…

THINNER COVERAGE BELOW

04 Identities & PATs inventory page for Azure DevOps NEW

55

A new Identities & PATs page inventories personal access tokens, service connections, and Entra service principals for Azure DevOps organizations in one place, with hourly auto-refresh, on-demand refresh, and per-tab export.

Review the new Identities & PATs inventory for your Azure DevOps organization to spot over-privileged or stale tokens, service connections, and Entra service principals at a glance.

📍 In the StepSecurity console, go to Identities & PATs (Azure DevOps), select the Personal Access Tokens tab, click Refresh to pull the latest data from the Azure DevOps APIs, then click Export to download the token inventory for that tab.

— UI navigation given but no API or config surface named

PAT Governance for GitHub and Azure Dev…

WAS THIS USEFUL? 👍 👎

Socket

Feedback ⓘ 1 RELEASE · 2026-09-01 BLOG ↗ RANK

Socket detects and blocks open source supply chain attacks by analyzing package dependencies for malicious code and security vulnerabilities.

> Socket launches Microsoft Teams as a full notification channel, letting teams route filtered, digested supply chain and vulnerability alerts as Adaptive Cards directly into Teams channels.

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

01 **Microsoft Teams notification channel** NEW 91

Socket adds Microsoft Teams as a notification destination configured under `Settings → Integrations → Notifications` via a Microsoft Workflows incoming webhook (HTTP POST URL), alongside the existing email channel. A new subscription model lets owners and admins route organization alerts and supply chain attack campaign notifications to specific Teams channels, filtered by alert category (supply chain risk, vulnerability, quality, maintenance, license), severity, Socket priority, repository, or package ecosystem. Notifications are delivered as structured Adaptive Cards summarizing alert totals by severity, affected repository count, individual finding previews, and a direct link to the Socket dashboard, with related alert activity grouped into digests to prevent channel flooding. Attack campaign notifications also indicate whether affected packages are present in the organization, showing impacted repositories or confirming none are affected without manual per-repository checks.

Connect a Teams channel to Socket so critical supply chain alerts land in your security team's channel automatically.

> 📍 In Socket, go to Settings → Integrations → Notifications → Create Channel, select `Microsoft Teams`, enter a channel name, and paste the HTTP POST URL copied from your Microsoft Workflows 'Post to a channel when a webhook request is received' flow. Socket will send a test Adaptive Card; a successful test marks the channel as Active.

Route only critical supply chain risk alerts for a specific repository to a dedicated engineering Teams channel, keeping noise out of the general security channel.

> 📍 In Socket, go to Settings → Integrations → Notifications → Create Subscription, choose the `alert created` event, set filters to category: `supply chain risk`, severity: critical, and the target repository, then select your Microsoft Teams channel as the destination.

— Full mechanism, config path, filters, and setup steps given. `launch-20260901-5d3aaad9`

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

ZeroPath

Feedback ⓘ 2 RELEASES · 2026-08-13 → 2026-08-20 BLOG ↗

RANK

AI-native SAST platform that finds 2x more real vulnerabilities with 75% fewer false positives. Automated vulnerability detection, instant fixes, and seamless CI/CD integration for modern DevOps teams.

> ZeroPath shipped reachability-aware SBOM/VEX/AI-BOM export and continuous CVE alerting that re-triages new advisories against existing SCA inventory within minutes.

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

01 Reachability-aware SBOM, VEX and AI-BOM export NEW

78

Adds SBOM export in `CycloneDX 1.6`, `SPDX 2.3`, standalone `CycloneDX VEX` documents, and AI-BOM formats, all generated from the same stored scan inventory. VEX statements are driven by reachability analysis and emit one of three machine-readable states — `not_affected` (with justification `code_not_reachable`), `exploitable`, or `in_triage` — instead of manually authored verdicts. The AI-BOM export is a CycloneDX ML-BOM covering seventeen AI component kinds (LLM SDKs, agent frameworks, vector databases, model weights, prompt templates, MCP servers) aligned to EU AI Act and NIST AI Risk Management Framework inventory expectations. License obligations are classified into five buckets — permissive, weak copyleft, strong copyleft, network copyleft (AGPL/Affero), and unknown — with network copyleft split out to surface AGPL's hosted-service trigger; packages with unknown licenses are marked `license-unknown` and fields with no data are omitted rather than filled with placeholders.

Generate a reachability-aware SBOM or standalone VEX document after running an SCA scan on a repository.

> 📍 In ZeroPath, open the repository, select `Generate SBOM`, then choose CycloneDX, SPDX, standalone VEX, or AI-BOM.

— Names formats and VEX states; only UI navigation given, no API launch-20260820-f30446d1

02 Continuous CVE alerting against SCA inventory NEW

78

When a fresh CVE lands on a direct dependency, ZeroPath automatically re-runs reachability and exploitability analysis — cloning the repo, checking whether the vulnerable function is actually called — and produces a triaged alert with reachability verdict, exploitability rating, confidence, severity, and a pointer to the relevant line. It

suppresses noise by hashing only the version-relevant portion of each OSV advisory (so cosmetic republications don't duplicate alerts), folds multiple hits from one CVE across many locations into a single notification, and enriches alerts with CISA KEV data and FIRST EPSS scores to surface reachable-and-actively-exploited findings first. Deep transitive dependency matches are recorded as `uninvestigated` rather than scored, and when a finding is exploitable with a safe upgrade available, the alert arrives with a pull request already attached. Alerting is opt-in per repository, tag, or organization, and can be routed to Slack, a webhook, or an agent playbook.

Enable continuous CVE alerting for a specific repository so your team is notified within minutes of a new advisory matching a shipped dependency — rather than waiting for the next scheduled scan.

> 📍 In the ZeroPath console, navigate to your repository settings, find the `Continuous CVE Alerting` section, and toggle it on. Optionally apply the setting at the tag or organization level to cover multiple repos at once.

Route continuous CVE alerts to a Slack channel or webhook endpoint so triage findings land directly in your team's workflow without polling the ZeroPath UI.

> 📍 In the ZeroPath console, go to Alert Destinations and add a Slack integration or webhook URL. New CVE alerts — already triaged with reachability and exploitability verdicts — will be posted there within minutes of an advisory hitting the OSV feed.

— Detailed mechanism and routing named; only console toggle steps, no API

`launch-20260813-542026be`

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

Truffle Security trufflehog

Feedback ⓘ

1 RELEASE · 2026-09-03 NOTES ↗ CODE ↗ RANK

trufflehog discovers, classifies, and validates leaked credentials

> TruffleHog's v3.97.4 release speeds up json-enumerator scanning with concurrent multi-file processing and native zstd support, plus reduces false positives in Twilio credential rotation checks.

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

01 Concurrent multi-file and zstd support in json-enumerator

IMPROVED 86

The `json-enumerator` source now supports passing multiple files at once, e.g. `trufflehog json-enumerator FILE_1 .. FILE_N`, replacing the previous sequential behaviour and improving throughput on multicore systems. It also adds native zstd-compressed NDJSON input handling, eliminating the need to decompress files externally before scanning, and `json-enumerator` can now be used inside a `multi-source` configuration.

Scan multiple zstd-compressed NDJSON files concurrently to maximize throughput on a multicore system without pre-decompressing them.

```
$ trufflehog json-enumerator secrets_dump_1.ndjson.zst
secrets_dump_2.ndjson.zst secrets_dump_3.ndjson.zst --
results=verified
```

— Names exact command, flags, formats, and config surface. v3.97.4

THINNER COVERAGE BELOW

02 Twilio detector treats transport errors as indeterminate

IMPROVED 55

Twilio and Twilio API key detectors now treat transport failures (429, 5xx, timeouts, connection resets, dial failures) as indeterminate rather than writing `date_rotated`, reducing false rotation signals on transient errors.

— Explains mechanism and named field but no direct user action. v3.97.4

WAS THIS USEFUL?  

infisical

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗ RANK

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

> Infisical v0.165.3 adds a Daytona secret sync integration, OIDC auth templates for Machine Identities, new PAM credential-access and session-liveness controls, and IdP-authoritative member profile syncing.

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

01 **Daytona secret sync integration** NEW 72

Adds a Daytona app connection and secret sync integration, enabling secrets stored in Infisical to be synced to Daytona environments. Configured via Project > Integrations > Secret Syncs by adding a sync, selecting Daytona, configuring the app connection, and choosing the source environment and path.

Configure a Daytona secret sync so secrets from an Infisical project environment are pushed to your Daytona workspace.

> 📍 In the Infisical console, go to your Project › Integrations › Secret Syncs, click Add Sync, select Daytona, configure the Daytona app connection, choose the source environment and path, then save.

— Names integration and gives exact setup steps v0.165.3

THINNER COVERAGE BELOW

02 **PAM credential access approval and session heartbeats** NEW 47

PAM account password viewing is now gated behind access requests, requiring an approval workflow before privileged account credentials are revealed. PAM also adds heartbeats to track liveness of privileged access sessions.

— Two PAM mechanisms described but no exact endpoints/flags v0.165.3

03 **OIDC auth templates for Machine Identities** NEW 45

Adds OIDC auth template support for Machine Identities, allowing reusable OIDC authentication configurations to be applied across multiple Machine Identities.

— Explains reuse mechanism but no config keys given v0.165.3

04 **IdP-authoritative member profile sync** NEW 40

Syncs member email and name from the identity provider when the IdP is configured as authoritative, keeping user profiles consistent with the upstream directory.

— Clear behaviour but no config surface named v0.165.3

05 **Policy delete endpoint opened to all plans** IMPROVED

40

Removes the plan-tier restriction from the policy delete endpoint, making policy deletion available regardless of subscription level.

— Names the endpoint area but not its path v0.165.3

06 **Human-readable names in approvals UI** IMPROVED

28

The approval UI now shows human-readable names instead of UUIDs in the approvals list.

— Simple UI tweak, exact change stated but minor v0.165.3

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

PortSwigger Burp Suite

Feedback ⓘ 1 RELEASE · 2026-09-03

BLOG ↗ RANK

We enable the world to secure the web. Burp Suite, the Web Security Academy, and world-leading research from PortSwigger â the AppSec communityâs home.

> Burp Suite DAST 2026.9 adds the ability to export issues as CSV directly from the Issues tab.

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

01 **CSV export of issues** NEW 50

The Issues tab now includes an option to download issues as a CSV file, enabling offline triage or reporting.

Export your current issue list to CSV for offline triage or reporting.

> 📍 In Burp Suite DAST, go to the Issues tab, then select the option to download issues as a CSV file.

— Names UI location and export format, no further mechanism given.

DAST 2026.9 (2026-09-03)

WAS THIS USEFUL? 👍 👎

Invicti

Feedback

1 RELEASE · 2026-09-03

BLOG ↗

RANK

Official documentation for Invicti AppSec Platform, Invicti Platform, and Invicti Enterprise — web application security testing, DAST, API security, and vulnerability management.

> Invicti's biggest window addition is automatic rate-limit-aware scan pacing with exponential backoff, alongside a major expansion of Agentic Pentesting (Vulnerability Chaining Agent, report exports, resource budgeting, recon document import) and new first-class Bearer Token/API Key authentication.

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

01 **SSL check bypass extended across scan-cli API calls** IMPROVED

83

Extends `INVICTI_IGNORE_SSL_CHECKS` in `scan-cli` to cover all outbound platform API calls during a scan — DAST, Inventory, Identity, and report/export endpoints — not just the ephemeral agent.

— Names the env var and every covered surface Release 20260903 (2026-09-03)

02 **Rate-limit-aware scan pacing with backoff** NEW

83

The scan engine now automatically throttles request pacing when rate-limiting response headers (`Retry-After` , `X-RateLimit-*`) are received, reducing false-negative risk and incomplete coverage on rate-limited targets, and applies exponential backoff with jitter when retrying requests that receive a 429 response with no `Retry-After` header.

— Names headers, status code, and retry mechanism precisely Release 20260903 (2026-09-03)

03 **Independent confidence threshold in scan-cli** IMPROVED

75

The `INVICTI_MINIMUM_CONFIDENCE` environment variable in `scan-cli` now independently fails a scan when the threshold is exceeded, without requiring `INVICTI_MINIMUM_SEVERITY` to also be set.

— Names exact env var and its new independent behavior Release 20260903 (2026-09-03)

04 **CI/CD script generator with no severity threshold** IMPROVED

75

Leaving the minimum severity field empty in the CI/CD script generator now produces a script with no minimum vulnerability threshold, applicable to Azure Pipelines, CircleCI, GitHub Actions, GitLab CI/CD, and Jenkins.

Generate a GitHub Actions CI/CD script with no minimum severity threshold so every finding is reported without a hard gate.

📍 In the Invicti AppSec Platform, go to Integrations › CI/CD Script Generator, select `GitHub Actions`, leave the `Minimum Severity` field empty, then click Generate Script.

— Names all five CI/CD targets and includes exact steps `product docs`

05 **Agentic Pentesting report export formats** NEW 65

Agentic Pentesting assessment reports can now be downloaded in Markdown (`.md`) and raw JSON formats, enabling import into automated pipelines and external tools.

— Names both formats and their pipeline use `Release 20260903 (2026-09-03)`

06 **Per-organization SCIM2 provisioning toggle** NEW 60

SCIM2 provisioning endpoints can now be toggled on or off per organization, preventing user and team updates or deletions through SCIM2-provisioned accounts when disabled.

— Explains behavior but not the exact toggle location `product docs`

07 **Assessment Profile resource budgeting** IMPROVED 60

Agentic Pentesting Assessment Profiles now support input caps, prioritization limits, and credit spend limits for more granular agent resource budgeting and control.

— Names the three limit types, not the UI path `Release 20260903 (2026-09-03)`

08 **First-class Bearer Token and API Key auth headers** NEW 60

Adds Bearer Token and API Key as dedicated, first-class authentication header types in target configuration, separate from functional headers, simplifying authenticated scan setup.

— Names the header types but not exact config field `Release 20260903 (2026-09-03)`

THINNER COVERAGE BELOW

09 **Scan schedules for applications and collections** NEW 55

Scan schedules can now be created for an entire application or collection, automatically running DAST scans across all included targets on a chosen recurrence.

— Describes scope and recurrence but no config path `product docs`

10 **Vulnerability Chaining Agent** NEW 55

A new Vulnerability Chaining Agent in the Agentic Pentesting assessment engine correlates individual findings to execute multi-step vulnerability chains, uncovering complex attack paths.

– Explains mechanism but stays high-level on operation Release 20260903 (2026-09-03)

11 **Secrets Manager credentials for IDOR/BOLA auth** NEW

55

Enables use of Invicti Secrets Manager credentials (API key, basic auth, bearer token) for IDOR/BOLA authentication configurations.

– Names credential types; screenshots show setup form Release 20260903 (2026-09-03)

12 **Recon agent document import for attack surface discovery** NEW

55

Enables the Recon agent to import architectural diagrams and documentation files (PDF, DOCX, MD) to discover non-crawlable attack surfaces.

– Names supported file types but not the import path Release 20260903 (2026-09-03)

13 **OCTO sitemap URL and parameter exclusions** NEW 55

Adds URL path and parameter exclusions to the OCTO sitemap in Agentic Pentesting, matching DAST scan exclusion capabilities.

– Names the exclusion types and comparison to DAST Release 20260903 (2026-09-03)

14 **Role Management permission visibility and WAF upload role** IMPROVED 55

Role Management now makes all permission group operations visible and configurable, giving administrators full control over custom role definitions, and assigns the WAF upload permission group to Security Manager, Administrator, and Account Owner roles.

– Names the roles granted the WAF upload permission Release 20260903 (2026-09-03)

15 **API target creation from API Catalog page** NEW 50

Adds the ability to create a new API target directly from the API Catalog page, with or without an API specification attached, without navigating to the Targets section first.

– Clear UI path but no config or endpoint named Release 20260903 (2026-09-03)

16 **Scanning agent Helm chart on OpenShift/ROSA** NEW 50

The scalable internal scanning agent Helm chart now supports deployment on OpenShift and Red Hat OpenShift Service on AWS (ROSA) clusters.

– Names platforms but no deployment steps given product docs

17 **DAST tech fingerprinting shared with Attack Agents** IMPROVED

50

Technologies and framework stacks detected by DAST scans are now automatically shared with Agentic Pentesting Attack Agents so exploit payloads are tailored to the target's actual technology stack.

– Clear mechanism but no configuration surface named `Release 20260903 (2026-09-03)`

18 **WebRTC chatbot detection** NEW 50

Adds WebRTC data channel (SDP) chatbot detection, extending chatbot analysis to applications using real-time communication protocols.

– Names the protocol detail but no usage steps `Release 20260903 (2026-09-03)`

19 **DAST Engine as distinct Attack Agents entry** IMPROVED 45

DAST Engine now appears as a distinct entry under Attack Agents, aligning vulnerability counts across AI agents and traditional DAST scans.

– States the UI change but little mechanism `product docs`

20 **Sitemap agent coverage visualization** NEW 45

Adds sitemap path-level and input-level agent coverage visualization, showing which endpoints were analyzed by scan-wide and input-specific agents.

– Describes what it shows but not where to view it `Release 20260903 (2026-09-03)`

21 **Agentic Pentest management in AppSec Platform UI** NEW 45

Enables management of Agentic Pentests directly from the AppSec Platform UI, with findings flowing into the same pipeline as standard DAST scans.

– States integration point but no navigation detail `Release 20260903 (2026-09-03)`

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Reverse Engineering

Vector 35 Binary Ninja

Feedback ⓘ 1 RELEASE · 2026-09-03

BLOG ↗ RANK

Binary Ninja is a modern reverse engineering platform with a scriptable and extensible decompiler.

> Binary Ninja 6.0 (Krypton) introduces a first-party MCP server for LLM integration, a new Binary Similarity diffing platform for Ultimate, TMS320C6x architecture support, and analysis that runs up to 2.16× faster while using up to 55% less peak memory.

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

01 Built-in MCP server for LLM integration NEW

95

Adds a built-in GUI MCP server, enabled via the `ui.mcp.enabled` setting (restart required) or `Plugins > MCP > Start Server`, listening at `http://127.0.0.1:24642/mcp` by default. The `ui.mcp.token` setting requires clients to send a matching bearer token, and `Plugins > MCP > Copy Connection Info` copies the exact URL and authorization header for the active session. A standalone `binaryninja_mcp` headless binary (stdio-based MCP server) is also shipped for Commercial and Ultimate on macOS and Linux.

Enable the MCP server on every launch so an LLM client (e.g. Claude Desktop) can always connect to your Binary Ninja session.

> 📍 In Binary Ninja, go to Settings, search for `ui.mcp.enabled`, and set it to true, then restart. Navigate to Plugins › MCP › Copy Connection Info to copy the URL and bearer token for your client config.

Restrict MCP access to authorised clients only by requiring a bearer token.

> 📍 In Binary Ninja Settings, search for `ui.mcp.token` and set it to a strong secret string. Clients must then include a matching `Authorization: Bearer <token>` header when connecting to `http://127.0.0.1:24642/mcp`.

— Exact settings, default URL, and commands given.

Binary Ninja 6.0 (Krypton) (2026-09-03)

02 Binary Similarity diffing platform (Ultimate) NEW

75

New Binary Similarity feature (Ultimate only) for comparing related binaries using pluggable providers, shipping with Google BinDiff and WARP providers, with automatic

annotation transfer between binaries. Exposed through Python, C++, and Rust APIs, enabling headless sessions and registration of custom providers and resolvers.

— Names providers and APIs but no exact usage steps.

Binary Ninja 6.0 (Krypton) (2026-09-03)

03 **Faster automated base address detection** NEW 60

Introduces a new BASE sampling mode (enabled by default) for faster automated base address detection, especially on large files; the previous IL Analysis Mode remains available for higher accuracy.

— Names both modes and describes default behaviour.

Binary Ninja 6.0 (Krypton) (2026-09-03)

THINNER COVERAGE BELOW

04 **AArch64 and MCP server added to free edition** NEW 55

Adds AArch64 (ARMv8) architecture and the MCP server to the free edition, plus a new Linux ARM64 build of the free version.

— Names architecture and new build target. Binary Ninja 6.0 (Krypton) (2026-09-03)

05 **Multiple global pointer registers per architecture** IMPROVED 50

Supports multiple independent global pointer registers per architecture (e.g. TriCore's four global data region pointers), improving decompilation of such targets.

— Explains mechanism with a concrete example architecture.

Binary Ninja 6.0 (Krypton) (2026-09-03)

06 **Refactored calling convention system** IMPROVED 50

Refactored calling convention system now properly represents structure parameters and return values, with new Go and Pascal calling conventions added.

— Names new conventions but no config or command. Binary Ninja 6.0 (Krypton) (2026-09-03)

07 **Faster analysis with lower memory use** IMPROVED 50

Analysis runs up to 2.16× faster and uses up to 55% less peak memory versus 5.3 across representative binaries.

— Concrete performance numbers but no actionable steps.

Binary Ninja 6.0 (Krypton) (2026-09-03)

08 **TMS320C6x DSP architecture support** NEW 45

Adds TMS320C6x (DSP) architecture support, bringing Ultimate to 19 first-party architectures.

— Names architecture and count, nothing further. Binary Ninja 6.0 (Krypton) (2026-09-03)

09 **HLIL_STRUCT_INITIALIZE IL operation** NEW 40

Adds `HLIL_STRUCT_INITIALIZE` IL operation for structure initializers in HLIL.

— Names the new IL operation, no usage example. Binary Ninja 6.0 (Krypton) (2026-09-03)

10 **Bundled Python upgraded to 3.13** IMPROVED 30

Upgrades the bundled Python to 3.13, now also included on Linux.

— Simple version bump, minimal detail. Binary Ninja 6.0 (Krypton) (2026-09-03)

11 **Extension Manager replaces Plugin Manager** IMPROVED 30

Replaces the Plugin Manager with a new Extension Manager UI.

— Names UI replacement without further mechanism. Binary Ninja 6.0 (Krypton) (2026-09-03)

12 **New user onboarding wizard** NEW 20

Adds a new user wizard to ease migration for new and upgrading users.

— Thin description with no specifics on wizard content.

Binary Ninja 6.0 (Krypton) (2026-09-03)

WAS THIS USEFUL?  

◆ Digital Forensics & Incident Response

ElcomSoft

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

Try professional password recovery, data decryption, mobile and cloud forensic tools from a manufacturer with 30+ years of expertise, providing tools and training to law enforcement, financial and intelligence agencies.

> ElcomSoft's Quick Triage update centers on a new unified Timeline view that merges multiple artifact types into one chronology, alongside a plugin-based artifact architecture adding six new artifact types, a lightweight file system snapshot capability, live-session BitLocker key extraction, and improvements to password recovery and full-text search.

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

01 Unified timeline view in Quick Triage NEW

80

A new Timeline view merges events from browser activity, network activity, recent files, Jump Lists, device activity, and program execution into a single chronology, presented as an event table and histogram with quick filtering, event cards, and jump-to-source-artifact links. Timeline exports to PDF and XLS.

Review the unified timeline to establish a chronological sequence of user activity across browser, USB, and program-execution artifacts during an investigation.

📍 In Elcomsoft Quick Triage 2.2, open your case project, then go to the Timeline view. Use the histogram to scope a time range of interest, type in the filter box to narrow events by keyword, and click any event card to jump directly to the source artifact (e.g., Prefetch or SRUM entry).

— Clear UI path with mechanism, but no CLI or config key. launch-20260903-ab424c6f

02 Plugin-based artifact architecture with six new artifact plugins

NEW

60

A new plugin-based artifact architecture enables six new artifact type plugins: Microsoft Defender logs, Windows Update Store (WUS), CAM database, Jump Lists, Windows Search index, and Prefetch files.

— Names six new artifacts but no usage steps given. launch-20260903-ab424c6f

THINNER COVERAGE BELOW

03 Automatic MSA hash attack in password recovery IMPROVED

55

Password recovery now automatically attempts an MSA hash attack with MSA-specific rules when the NTLM hash yields no result, including MSA hash extraction.

— Explains the trigger logic but gives no usage steps. `launch-20260903-ab424c6f`

04 **Full-text search parses OpenDocument files and nested archives**

IMPROVED

53

Full-text search now parses OpenDocument files (`.odt` , `.ods` , `.odp`) and recursively parses nested archives up to 10 levels deep.

— Names formats and depth limit but no steps. `launch-20260903-ab424c6f`

WAS THIS USEFUL? 👍 👎

Belkasoft

Feedback ⓘ 1 RELEASE · 2026-09-02 BLOG ↗ RANK

Accelerate your digital forensics and incident response investigations with Belkasoft

> Belkasoft X 2.12 introduces offline AI capabilities via BelkaGPT — evidence translation, SQLite database classification, and a distributed processing hub — alongside a local offline map server, a redesigned MTK Dump acquisition workflow with new chipset support, and expanded Windows, Android, and iOS artifact extraction.

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

01 **Redesigned MTK Dump acquisition workflow** IMPROVED 95

The MTK Dump acquisition workflow now separates acquisition and decryption into independent operations and adds passcode brute-force with unknown-length support, dictionary-based alphanumeric attacks, and new chipset support: `MT3369`, `MT6762`, `MT6880`, `MT6883`, `MT6889`, `MT6890`, `MT8765`, `MT8766B`, and `MT8768T`. Investigators can run acquisition to capture a raw dump, then later return to the saved dump and select Decrypt user data partition to enter a known passcode or launch a dictionary-based brute-force attack.

Acquire a MediaTek device and defer decryption until a passcode is obtained or a dictionary attack can be staged.

> 📍 In the MTK Dump acquisition workflow, run acquisition to capture the raw dump, then return to the saved dump later and select Decrypt user data partition — entering a known passcode or launching a dictionary-based brute-force attack against alphanumeric passwords.

— Named chipsets and exact decrypt workflow steps launch-20260902-a2cac212

02 **Belkasoft Offline Map Server** NEW 90

The Belkasoft Offline Map Server is a locally deployed map server for reviewing geolocation evidence without connecting forensic workstations to online mapping services, configured by specifying its network address in Belkasoft X settings. To use it, download the required map tiles, deploy the server within your network, then enter its network address under Settings in Belkasoft X to enable offline map review.

Review geolocation evidence on maps in an air-gapped forensic lab by pointing Belkasoft X at an internal map server.

> 📍 Download required map tiles, deploy Belkasoft Offline Map Server within your network, then in Belkasoft X go to Settings and enter the server's network address to enable offline map review.

– Exact setup steps and config location given launch-20260902-a2cac212

03 **Windows artifact extraction expansions** NEW 75

Belkasoft X extends Windows artifact support in several areas: BAM/DAM artifact extraction now covers Windows 10 version 1809 and later, capturing executable paths and timestamps from Background Activity Moderator and Desktop Activity Moderator data; a new Remote Desktop Cache reconstruction feature extracts Windows Remote Desktop bitmap cache tiles and automatically combines visually matching fragments into larger image sequences; a new SRUM (System Resource Usage Monitor) artifact extraction parses historical application network activity and associated timestamps; and System Event Log artifacts gain an Event cluster property that groups events into activity categories such as system logon/logout, software installation, remote access, Wi-Fi connections, and system startup/shutdown.

– Names all four artifacts and fields, no exact UI path launch-20260902-a2cac212

04 **Custom SQLite artifact mapping** NEW 70

Custom SQLite artifacts let investigators map tables and columns from unsupported databases to standard Belkasoft X artifact fields (timestamps, participant names, message text, identifiers, geolocation) for search, filter, review, and reporting alongside parsed evidence.

– Details mapped fields, no exact workflow steps launch-20260902-a2cac212

05 **Android agent-based acquisition via USB and custom folders** IMPROVED 65

The Android agent-based acquisition (Agent backup via SD card method) now supports USB flash drives via USB-C adapters, custom folder selection on device or external media, and improved reliability on recent Android versions with added SMS and call history collection.

– Names method and additions but no exact steps launch-20260902-a2cac212

06 **Improved extraction for existing Android apps** IMPROVED 65

Belkasoft X improves extraction for Android apps including Facebook (contact info, chat threads), Instagram (threads and reactions), Telegram (account owner name, replies, reactions, service messages, call duration), Viber (replies, reactions, call duration, picture captions), WhatsApp (contact merging, reply visualization, vCard contacts), and X/Twitter (separated DMs/group chats from feed, pictures, voice messages, reactions).

– Details what each app extraction gained, no steps launch-20260902-a2cac212

07 **BelkaGPT Hub installer for distributed AI processing** NEW 60

The new `BelkaGPT Hub installer for Windows` simplifies deployment of distributed offline AI processing to GPU-equipped workstations and servers in a local network, with selectable GPU and CPU resources.

— Names installer and resource selection but no exact deployment steps

launch-20260902-a2cac212

---

08 **iOS app support and extraction improvements** IMPROVED

60

Belkasoft X adds iOS support for ChatGPT v1.2026.160 and improves extraction for Apple Unified Logs (application names in Timeline Info field), Instagram, WeChat (messages, reactions, media), and Zalo (audio artifacts).

— Names apps and specific fields, no workflow steps launch-20260902-a2cac212

THINNER COVERAGE BELOW

09 **New Android app support** NEW

50

Belkasoft X adds support for new Android applications including Burner, FairEmail, Google Play (`library.db`), Google Quick Search Box, Google Voice, GroupMe, Life360, Mastodon, MeWe, Microsoft Teams, TeleGuard, Waze, and Wire.

— Lists apps added but no extraction detail per app launch-20260902-a2cac212

10 **RSMF 2.0 export support and splitting** NEW

40

Belkasoft X adds support for the `RSMF 2.0` format and export splitting for large datasets.

— Names format version, no detail on split mechanics launch-20260902-a2cac212

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Fastly

Feedback ⓘ 2 RELEASES · 2026-09-03 BLOG ↗ RANK

Fastly is a content delivery network and edge computing platform that accelerates website and application performance globally.

> Fastly shipped a batch of Go and JavaScript Compute SDK updates, headlined by new TLS SNI visibility for edge logic and richer request metadata, dynamic backend healthchecks, and finer shielding timeouts in the Go SDK.

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

01 **clientSNI property on FetchEvent.client** NEW 80

The JavaScript SDK adds a `clientSNI` property to `FetchEvent.client`, exposing the TLS Server Name Indication value from the incoming client connection at the edge, enabling routing or logging based on the SNI hostname without inspecting the Host header.

Route or log based on the SNI hostname the client presented during TLS handshake, enabling per-domain edge logic without inspecting the Host header.

javascript

```
addEventListener('fetch', (event) => {
  const sni = event.client.clientSNI;
  if (sni === 'api.example.com') {
    // apply API-specific logic
  }
  event.respondWith(fetch(event.request));
});
```

— Named property plus a runnable code example demonstrating use.

JavaScript SDK 3.45.0 (2026-09-03)

THINNER COVERAGE BELOW

02 **ComplianceRegion and RawHeaders fields on FastlyMeta** NEW 55

The Go SDK's `fsthttp` package adds `ComplianceRegion` and `RawHeaders` fields to `FastlyMeta`, giving compute programs richer access to request metadata.

— Names exact fields and package but no usage example. Go SDK 1.10.0 (2026-09-03)

03 **SendErrorDetailTag export in fsthttp** NEW 50

The Go SDK exports `SendErrorDetailTag` from the `fsthttp` package for programmatic error detail handling.

— Names exact exported symbol and package. Go SDK 1.10.0 (2026-09-03)

04 **Optional removal of net/http support for leaner builds**

IMPROVED

50

The Go SDK allows removing support for `net/http` in the `fsthttp` package, enabling leaner builds.

— Names exact package and build benefit, no migration steps given.

Go SDK 1.10.0 (2026-09-03)

05 **Shielding package first-byte and between-bytes timeouts** NEW

45

The Go SDK's `shielding` package gains first-byte and between-bytes timeouts.

— Names package and timeout types, no config example. Go SDK 1.10.0 (2026-09-03)

06 **Dynamic backend healthchecks in Go SDK** NEW

40

The `fsthttp` package now supports dynamic backend healthchecks.

— States capability but no mechanism or config detail. Go SDK 1.10.0 (2026-09-03)

WAS THIS USEFUL?  

CLOUD & CONTAINER SECURITY

◆ CNAPP

Zscaler Posture Control

Feedback ⓘ 1 RELEASE · 2026-09-04

BLOG ↗ RANK

Zscaler Posture Control monitors and enforces security compliance policies across devices and users in cloud and on-premises environments.

> Zscaler Posture Control gains an AI-driven Endpoint AI Security Attack Chain Analysis capability that reasons across full endpoint state to produce prioritized, step-by-step remediation roadmaps.

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

01 **Endpoint AI Security Attack Chain Analysis** NEW 60

A new Endpoint AI Security Attack Chain Analysis capability reasons over the full state of an endpoint — AI agents, coding assistants, IDE and browser extensions, installed software, packages, and system configuration — to construct a realistic, step-by-step attack chain rather than a flat list of findings. Each step in the output is labeled as confirmed on the host, inferred from state, or flagged for verification, and the tool produces a prioritized remediation roadmap ordered by attacker progression. It runs as an endpoint agent, either standalone or as a module within the existing Zscaler client (deployed on more than 70 million devices), and is fully controlled and policy-scoped.

— Clear mechanism and scope described but no config/API surface named.

2026-09-04-3a6c7ef8

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

Cloud Custodian

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗

CODE ↗ RANK

Rules engine for cloud security, cost optimization, and governance, DSL in yaml for policies to query, filter, and take actions on resources

> Cloud Custodian 0.9.52 adds more than 40 new AWS, Azure and GCP resources, filters and actions spanning Bedrock, Vertex AI, VPC endpoints, DNS management, Clean Rooms, SageMaker Studio and more, plus a breaking field rename in c7n-org account configuration.

└──▷ WHAT SHIPPED · 38 FEATURES most completely described first ? what's the number?

01 **GCP DNS policy and DNSSEC management actions** NEW 79

Adds an `update` action to `gcp.dns-policy` resources and `enable-dnssec` / `set-dnssec-key-specs` actions to `gcp.dns-managed-zone`.

Enable DNSSEC on all GCP managed zones that do not yet have it, enforcing DNS integrity at scale.

yaml

```yaml
policies:
  - name: enforce-dnssec-on-managed-zones
    resource: gcp.dns-managed-zone
    filters:
      - type: value
        key: dnssecConfig.state
        value: "on"
        op: ne
    actions:
      - type: enable-dnssec
```

— Runnable YAML policy enforcing DNSSEC provided 0.9.52.0

02 **VPC endpoint delete and cross-region inspection** NEW 78

Adds a `delete` action to `aws.vpc-endpoint` resources, enabling policy-driven removal of unwanted VPC endpoints, and a `service-details` filter for cross-region endpoint inspection.

Delete idle VPC endpoints tagged for a specific service to reduce attack surface and cut PrivateLink costs.

```yaml
policies:
  - name: delete-unused-aoss-vpc-endpoints
    resource: aws.vpc-endpoint
    filters:
      - type: value
        key: ServiceName
        op: contains
        value: "aoss"
    actions:
      - type: delete
```

— Runnable YAML policy example provided `0.9.52.0`

03 **Bedrock job and inference management actions** NEW 71

Adds `tagging`, `mark-for-op`, and `stop` actions to `aws.bedrock-model-invocation-job` and `aws.bedrock-inference-profile` resources, a metrics filter to `aws.bedrock-agent`, a synthetic total-tokens metric on `aws.bedrock-inference-profile`, and new `aws.bedrock-evaluation-job` and `aws.bedrock-mantle-project` resources.

— Names every action and resource but no example shown `0.9.52.0`

04 **Azure AI Foundry and Machine Learning resources** NEW 62

Adds `azure.ai-foundry-agent`, `azure.ai-foundry-application`, and `azure.cognitiveservice-deployment` resources with actions, plus `azure.machine-learning-job` (with an `archive` action), `azure.machine-learning-online-endpoint`, `azure.machine-learning-model-version`, and `azure.machine-learning-data-container` resources.

— Enumerates all named resources, no example `0.9.52.0`

05 **Dormant KMS key detection filter** NEW 61

Adds a `last-usage` filter to `aws.kms-key` resources for identifying dormant keys.

Flag KMS keys that have not been used recently so they can be reviewed and scheduled for deletion.

```yaml
policies:
  - name: flag-dormant-kms-keys
    resource: aws.kms-key
    filters:
      - type: last-usage
        value: 90
        op: greater-than
        value_type: age
    actions:
      - type: mark-for-op
        op: disable
        days: 7
```

— Runnable YAML example flags and disables dormant keys `0.9.52.0`

06 **Vertex AI resource and job support** NEW 60

Adds a `monitor` action and metrics filter to `gcp.vertex-ai-endpoint`, and new resources `gcp.vertex-ai-custom-job`, `gcp.vertex-ai-dataset`, `gcp.vertex-ai-hyper-parameter-tuning-job`, `gcp.vertex-ai-model`, and `gcp.vertex-ai-evaluation-run`.

— Names all resources; no usage example given `0.9.52.0`

THINNER COVERAGE BELOW

07 **Payment Cryptography account and cross-account filters** NEW 55

Adds a `payment-cryptography-replication-regions` filter on the `aws.account` resource and a cross-account filter to `aws.payment-cryptography` resources.

— Named filters, no example or scope detail `0.9.52.0`

08 **AWS Clean Rooms resource support** NEW 52

Adds a `members` filter to `aws.cleanrooms` collaboration resource and new `aws.cleanrooms` and `aws.cleanrooms-ml` resources.

— Named resource and filter, no example `0.9.52.0`

09 **c7n-org accounts Status field renamed to State** BREAKING 50

In `aws.c7n-org` accounts configuration, the `Status` field for retiring accounts is renamed to `State`.

— Names exact field rename but no migration example `0.9.52.0`

10 **Delete action for WAF Classic Web ACLs** NEW 48

Adds a `delete` action for `aws.waf` and `aws.waf-regional` Classic Web ACLs.

— Named action and resources, no example `0.9.52.0`

11 **Allow-all detection in list-form IAM policies** NEW 48

Adds `has-allow-all` detection for list-form `Action` / `Resource` entries in `aws.iam-policy`.

— Describes specific detection logic, no example `0.9.52.0`

12 **Resource lookup in tag values for AWS and Azure** NEW 47

Adds resource lookup support in tag values for `aws.tags` actions, enabling dynamic tag propagation, and the same resource lookup support in tag values for Azure `tags` actions.

— Cross-cloud mechanism named, no example config `0.9.52.0`

13 **Entra ID auth for Azure Function App operations** BREAKING 43

Replaces SCM basic auth with Entra ID bearer token for `azure.function-app` operations.

— Names old and new auth mechanism, no migration steps `0.9.52.0`

14 **EC2 rightsizing recommendations filter** NEW 42

Adds a `compute-optimizer` filter to `aws.ec2` resources for rightsizing recommendations.

— Names purpose but no example or config `0.9.52.0`

15 **SageMaker Studio resource support** NEW 40

Adds new `aws.sagemaker-studio` app, user-profile, and space resources.

— Bare resource names, no mechanism detail `0.9.52.0`

16 **MemoryDB parameter group support** NEW 40

Adds a `db-parameter` filter and a new `aws.memorydb-parameter-group` resource.

— Two named surfaces, no usage shown `0.9.52.0`

17 **GCP metrics filter missing-value handling fix** IMPROVED 40

Extends the `gcp.metrics` filter to honor `missing-value: 0` correctly.

— Names exact config value fixed, no example `0.9.52.0`

---

18 **OpenSearch domain config update action** NEW 39

Adds `update-domain-config` action to `aws.elasticsearch` (OpenSearch) domains.

— Named action, no example given `0.9.52.0`

---

19 **CloudFront function and key-value store resources** NEW 38

Adds new `aws.cloudfront-function` and `aws.cloudfront-keyvalue-store` resources.

— Two named resources, no further detail `0.9.52.0`

---

20 **Notebook v2 resource with metadata actions** NEW 37

Adds new `gcp.notebook-v2` resource with `get` and `update-metadata` actions.

— Names resource and its actions, no example `0.9.52.0`

---

21 **Org-unit whitelisting in cross-account filter** NEW 35

Adds org-unit whitelisting to the cross-account filter across AWS resources.

— General scope, no named parameter or example `0.9.52.0`

---

22 **QuickSight subscription and permissions filters** NEW 35

Adds `aws.quicksight` account subscription and custom permissions filters.

— Named resource, filters not individually named `0.9.52.0`

---

23 **Matched security rule annotation for Azure NSGs** IMPROVED 35

Adds matched-security-rule annotation to Azure NSG ingress/egress filters.

— Describes annotation behaviour, no example `0.9.52.0`

---

24 **Service quota fields expansion** IMPROVED 33

Adds `Services` and `DefaultServiceQuotas` to `aws.service-quota` resource via `quota.py`.

— Names fields and file, no usage example `0.9.52.0`

---

25 **EMR termination policy filter** NEW 32

Adds a `termination-policy` filter to `aws.emr` clusters.

— Bare filter name, no example `0.9.52.0`

---

26 **Mark-for-op support for CloudFormation stacks** NEW

32

Adds `mark-for-op` support to `aws.cfn` (CloudFormation stack) resources.

— Named action, no example `0.9.52.0`

---

27 **SNS topic resolution by ARN in CloudTrail mode** IMPROVED

32

Adds SNS topic resolution directly by ARN in CloudTrail event mode.

— Describes mechanism briefly, no example `0.9.52.0`

---

28 **GCP audit mode for API keys** NEW

30

Adds `gcp-audit` mode support to `gcp.api-key` resources.

— Named mode, no mechanism explained `0.9.52.0`

---

29 **Regional persistent disk support for GCP disk actions**

IMPROVED

30

Adds regional persistent disk support for GCP disk actions.

— Generic description, no action or field named `0.9.52.0`

---

30 **Azure private DNS resource support** NEW

29

Adds `azure.private-dns-zone` and `azure.private-dns-record-set` resources.

— Two named resources, no actions listed `0.9.52.0`

---

31 **Security Hub master account filter** NEW

28

Adds a `master` filter to `aws.security-hub` resource.

— Bare filter name, minimal detail `0.9.52.0`

---

32 **Server-side encryption for S3 policy logs** NEW

28

Adds configurable server-side encryption for S3 policy log output.

— No config key named, generic description `0.9.52.0`

---

33 **BigQuery dataset update action** NEW

28

Adds `update` action to `gcp.bq-dataset` resources.

— Named action only, no example `0.9.52.0`

---

34 **Aurora DSQL resource support** NEW

26

Adds new `aws.dsql` (Aurora DSQL) resource support.

— Bare new resource, no filters/actions listed 0.9.52.0

35 **Compute instance metadata support** IMPROVED 24

Adds compute instance metadata support for `gcp.instance` resources.

— Generic description, no field or filter named 0.9.52.0

36 **VPC Lattice rule resource** NEW 21

Adds new `aws.vpc-lattice-rule` resource.

— Bare resource name only 0.9.52.0

37 **Azure budget resource** NEW 18

Adds `azure.budget` resource.

— Bare resource name, no further detail 0.9.52.0

38 **GCP regional commitment resource** NEW 18

Adds new `gcp.regional-commitment` resource.

— Bare resource name only 0.9.52.0

└──▷ **BREAKING ON UPGRADE**

! In `aws.c7n-org` accounts configuration, the `Status` field for retiring accounts is renamed to `State`.

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

calico

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

Cloud native networking and network security

> Calico's biggest move this window is Mylo, an AI-agent layer exposed through a new Calico MCP Server that lets any MCP-compatible AI agent diagnose Kubernetes network and policy issues without a bespoke chat UI.

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

01 **Calico MCP Server for AI agent access** NEW 75

Introduces the Calico MCP Server, which exposes Mylo's tools and skills to any MCP-compatible AI agent (Claude, Cursor, terminal agents, etc.) without requiring a new chat interface. Supports two run modes: live cluster diagnostics via the existing `kubeconfig` path (compatible with `kubectl` and `calicoctl`) for real-time use, and a fully offline mode against a Calico diagnostics bundle for air-gapped or post-incident analysis.

— Names the server, agents, and both run paths but no runnable command launch-20260903-19c8abe9

02 **diagnose_connectivity trace tool** NEW 65

Adds the `diagnose_connectivity` tool via the MCP Server, which returns an ordered, opinionated trace of a network path down to the specific Calico policy rule allowing or denying traffic, along with a suggested fix, rather than a raw dump.

— Named tool with clear mechanism but no invocation syntax shown launch-20260903-19c8abe9

THINNER COVERAGE BELOW

03 **Packaged troubleshooting skills for agents** NEW 40

Packages multi-step troubleshooting workflows (skills) — including connectivity failure triage, policy review before deployment, and incident triage — as structured, agent-callable procedures encoding Tigera's operational expertise.

— Lists skill types but no detail on invoking or extending them launch-20260903-19c8abe9

04 **Scoped request router in Mylo** NEW 35

Includes a built-in router that explicitly scopes each agent request to what Mylo can handle, preventing silent CLI fallback when a request falls outside its lane.

— Explains purpose but no mechanism detail beyond a design principle

launch-20260903-19c8abe9

WAS THIS USEFUL? 👍 👎

Docker Compose

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗

RANK

Define and run multi-container applications with Docker

> Docker Compose v5.5.1 improves debugging visibility, surfacing OpenTelemetry shutdown errors and lifecycle hook output directly in Compose's own output.

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

01 OpenTelemetry shutdown errors surfaced via --debug

IMPROVED

55

Running Compose with `--debug` now surfaces OpenTelemetry shutdown errors, making tracing misconfiguration visible instead of being silently swallowed.

— Names the exact flag but no further mechanism detail v5.5.1

02 Lifecycle hook output captured in Compose output

IMPROVED

38

Compose now captures and surfaces lifecycle hook stdout/stderr directly in its own output, so pre/post hook activity is visible without digging into container logs.

— Describes behaviour change but no named flag or config key v5.5.1

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Iru

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗ RANK

Manage devices and everything they touch. See how security, IT, and compliance get easier when unified around devices with Iru.

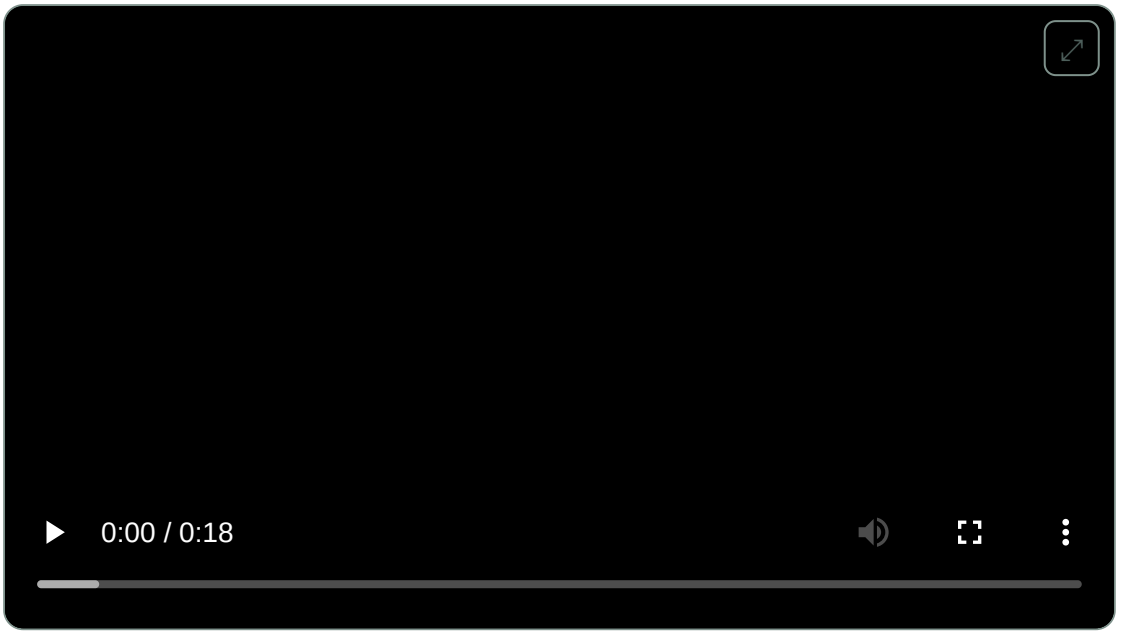
> Iru added automatic retry enrollment for Return to Service erasures, letting compatible iOS/iPadOS devices reattempt enrollment on their own if the first post-erase attempt fails.

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

01 Automatic retry enrollment for Return to Service NEW

70

A new Retry enrollment option, checked by default, appears inside the Erase device modal when Use Return to Service is enabled. It lets iPhone and iPad running iOS 27 or iPadOS 27 later automatically reattempt enrollment if the initial post-erase enrollment attempt fails, without manual intervention.



Re-enroll a wiped device without manual intervention when the first enrollment attempt fails after a Return to Service erase.

📍 In the Erase device modal, check Use Return to Service, then confirm Retry enrollment is checked (on by default) before submitting — applies to iPhone/iPad running iOS 27 or iPadOS 27 or later.

— Names exact modal, flag, default state and OS versions; no info on retry limits/timing.

Automatic retry enrollment for Return t…

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

OpenCTI

Feedback ⓘ 1 RELEASE · 2026-09-04 NOTES ↗ RANK

Open Cyber Threat Intelligence Platform

> OpenCTI strengthened session security by deriving session signature keys from the platform's existing app encryption key.

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

01 **Session signature key derived from encryption key** IMPROVED

45

The session signature key is now derived from the app's encryption key, tying session integrity to the platform's existing encryption configuration rather than a separate secret.

— Explains mechanism but no config key or migration steps given. 7.260904.0

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Axonius

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

Axonius is a cyber asset management platform that discovers, inventories, and manages all devices and software across an organization's IT infrastructure.

> Axonius 9.0.6 introduces a Jira ticketing flow launchable from asset queries and Recommended Actions, extends Risk Score configuration to sub-assets, adds Okta Universal Logout support, ships three new adapters, and expands enrichment, authentication, and filtering options across a wide range of existing adapters.

└──▷ **WHAT SHIPPED · 24 FEATURES** most completely described first ? what's the number?

01 **Application Settings fetching added to Datadog, Elasticsearch, Keycloak, Harness, and Dell Boomi adapters**

NEW 85

Adds Fetch Application Settings advanced settings to the Datadog, Elasticsearch, Keycloak, and Harness adapters, and a new Account ID connection setting to Dell Boomi (existing connections without an Account ID continue to fetch only Devices data). Datadog fetches account-, user-, and role-level settings including ownership, domain and IP allowlists, governance notifications, identity providers, roles, sensitive-data scanning, and user settings; Elasticsearch fetches cluster settings, API keys, users, and security settings; Keycloak fetches realm settings and user-profile settings; Harness fetches authentication mechanisms, role assignments, LDAP configuration, session timeouts, and security policies; and Dell Boomi exposes authentication methods, user privileges, and SCIM provisioning status as a new Application Settings asset type. All results are stored as Application Settings assets.

— Names every setting and data fetched per adapter

Axonius Release Notes 9.0.6 (2026-09-03)

02 **Configurable supported OS version window** NEW 83

Adds Number of Supported Major OS Versions setting under Settings > Enrichment, which controls how many recent major OS versions are considered supported per OS type and populates the Is Supported OS Version Device field (default: one supported major version per OS type).

Define how many recent major OS versions are treated as supported so the Is Supported OS Version Device field reflects your organisation's patching policy.

📍 In Axonius, go to Settings › Enrichment, locate Number of Supported Major OS Versions, and set the value for each OS type you want to override (default is 1).

— Named config key, default value, resulting field, and example

Axonius Release Notes 9.0.6 (2026-09-03)

03 **Saviynt account and entitlement fetching** NEW 83

Adds the option to fetch Saviynt accounts as Account/Tenant assets from the `getAccounts` endpoint, with optional filtering to Active status, and entitlement details per user from the `getEntDetailsforUsers` endpoint.

— Names both source endpoints and resulting asset type

Axonius Release Notes 9.0.6 (2026-09-03)

04 **HPE Aruba Networking Central Gateway support and details** NEW 82

Adds Gateway as a selectable option in the HPE Aruba Networking Central Devices type to fetch advanced setting, with configurable concurrent gateway detail requests (1–25) and a new API rate limit setting (max calls per second). Also adds an option to fetch extended Gateway details (serial number, model, OS, status, group name, uplink), consuming one additional API call per Gateway.

— Names every setting, range, and per-call cost Axonius Release Notes 9.0.6 (2026-09-03)

05 **Cisco Catalyst Center license fetching** NEW 80

Adds Fetch Licenses advanced setting to the Cisco Catalyst Center adapter, creating License assets and enriching device records with expiry status, feature license details, and Smart Account pool usage metrics.

Fetch Cisco Catalyst Center license compliance and Smart Account pool metrics alongside device inventory.

> 📍 In the Cisco Catalyst Center adapter settings, open Advanced Settings and enable Fetch Licenses. On the next discovery cycle, License assets appear and device records are enriched with expiry status, feature license details, and account pool metrics.

— Named setting, resulting asset type, and enrichment fields

Axonius Release Notes 9.0.6 (2026-09-03)

06 **Network Routes enrichment controls** NEW 78

Adds two new global Network Routes enrichment settings under Settings: Network Routes Enrichment (enables/disables the enrichment pipeline during discovery cycles) and Zones to Exclude (names of zones whose subnets are excluded from enrichment).

Exclude noisy internal zones from Network Routes enrichment to reduce discovery cycle overhead.

📍 In Axonius, go to Settings › Network Routes, enable `Network Routes Enrichment`, and enter zone names (e.g. `DMZ`, `Lab`) in the `Zones to Exclude` field.

— Exact config keys, location, and a usage example

Axonius Release Notes 9.0.6 (2026-09-03)

---

07 **ServiceNow custom parsing rules replace operational status setting**

78

BREAKING

Replaces the ServiceNow `Parse operational status` advanced setting with configurable `Custom Parsing rules`; existing enabled configurations are automatically migrated to two equivalent rules covering Operational Status and Asset Operational Status fields.

— Names old and new settings plus migration behaviour

Axonius Release Notes 9.0.6 (2026-09-03)

---

08 **Jira ticketing from asset queries and Recommended Actions**

NEW

75

A new ticketing flow lets users open one or more Jira tickets directly from selected assets or an entire query result, with content pre-filled from asset data, a rich-text editor supporting dynamic value tokens, a live ticket count preview, and a Test Tickets option against a single sample asset. The flow is also available from the Recommended Actions page, with controls to include or exclude specific groups of Security Findings (e.g. those missing ownership data) and to group findings by one or more asset fields to control ticket count.

— Mechanism and UI controls described but no exact navigation path

Axonius Release Notes 9.0.6 (2026-09-03)

---

09 **Alternative authentication methods across four adapters** NEW

75

Adds JWT Token authentication (OAuth2 Client ID and Client Secret) as an alternative to API Key in the RUCKUS Cloud adapter, OAuth 2.0 Client Credentials as an alternative to API Key in the BeyondTrust Password Safe adapter, API Key authentication as an alternative to username/password for the Check Point Infinity adapter when connecting to a Management Server, and ISPSS authentication support (Identity Administration sub-domain and EPM API application alias) for the CyberArk Endpoint Privilege Manager adapter.

— Names each adapter and its exact new auth mechanism

Axonius Release Notes 9.0.6 (2026-09-03)

10 **Cisco Firepower Management Center ARP table fetch removed** 70

BREAKING

The Cisco Firepower Management Center adapter no longer fetches ARP table data from firewall devices; the `Fetch ARP table from firewall devices` advanced setting has been removed. Access and NAT firewall rule assets no longer include a policy device name in their asset ID or firewall name.

— Names removed setting and downstream asset ID impact

Axonius Release Notes 9.0.6 (2026-09-03)

---

11 **Risk Score configuration for sub-assets** NEW 67

Enables Risk Score configuration for sub-assets (e.g. Network Devices, Repositories); when both a sub-asset and its parent asset have a Risk Score configured for the same asset or Security Finding, the sub-asset score takes precedence.

— Precedence rule explained but no config path given

Axonius Release Notes 9.0.6 (2026-09-03)

---

12 **Three new adapters: DataDome, Zentral, Zero Touch** NEW 60

Adds three new adapters: DataDome (bot protection, fetches Business Applications and Firewalls), Zentral (endpoint visibility for Apple/Linux/Android, fetches Devices and Users), and Zero Touch (unified endpoint management, fetches Devices).

— Names each adapter and asset types but no config detail

Axonius Release Notes 9.0.6 (2026-09-03)

---

13 **Entra ID / Intune Last Sign-In fetch options** NEW 60

Adds two new options to the Microsoft Entra ID / Intune `Fetch users Last Sign-In - How to fetch` advanced setting: non-interactive sign-ins (token refreshes, background service authentications) and automated processes.

— Named setting and both new option values Axonius Release Notes 9.0.6 (2026-09-03)

---

14 **Arnica.io repository fetch via direct endpoint** IMPROVED 60

Updates the Arnica.io adapter to retrieve repository information directly from the `/v1/inventory/repos` endpoint instead of aggregating it from findings data.

— Names endpoint and describes before/after data source

Axonius Release Notes 9.0.6 (2026-09-03)

THINNER COVERAGE BELOW

15 **Okta Universal Logout support** NEW 57

Adds Okta Universal Logout support, enabling Okta Identity Threat Protection (ITP) to immediately terminate active Axonius user sessions on detected security risks such as compromised credentials or session hijacking.

– Explains trigger and effect but no setup steps Axonius Release Notes 9.0.6 (2026-09-03)

16 **New dynamic charts on remediation pages** NEW 55

Adds dynamic charts to the Remediation Ownership page showing Security Findings per owner and Owned vs. Unowned Security Findings distribution, and to the Recommended Actions page showing actions per remediation owner and distribution of action sub-types.

– Chart contents named but no navigation or interaction detail

Axonius Release Notes 9.0.6 (2026-09-03)

17 **HPE OneView fallback device manufacturer** NEW 53

Adds HPE fallback Device Manufacturer value advanced setting and Device Manufacturer population from physical server chassis data to the HPE OneView adapter.

– Names the setting and data source but limited detail

Axonius Release Notes 9.0.6 (2026-09-03)

18 **IFS Assyst business applications parsing setting** NEW 53

Adds Parse Records with Status Name Starting with 'App' as Business Applications advanced setting to the IFS Assyst adapter.

– Full setting name given, no further behaviour detail

Axonius Release Notes 9.0.6 (2026-09-03)

19 **FortiDLP State field and Last Seen exclusion** NEW 53

Adds the State field (active or archived) and a new advanced setting to exclude devices with no or empty Last Seen value to the FortiDLP adapter.

– Names field and setting but limited mechanism Axonius Release Notes 9.0.6 (2026-09-03)

20 **CrowdStrike Falcon setting renamed** BREAKING 53

The CrowdStrike Falcon advanced setting Enrich Configuration Assessment with Rule Name is renamed to Enrich Configuration Assessment with Rule Information; any saved references to the old name must be updated.

– Names both old and new setting for direct migration

Axonius Release Notes 9.0.6 (2026-09-03)

21 **GCP Artifact Registry repositories as Compute Services** NEW 50

Adds option to fetch Google Cloud Artifact Registry repositories as Compute Services assets in the GCP adapter.

— Names the source and resulting asset type only Axonius Release Notes 9.0.6 (2026-09-03)

22 **DNSFilter Organization ID filter** NEW 45

Adds option to filter fetched devices by Organization ID in the DNSFilter adapter.

— Single-line addition with no further mechanism Axonius Release Notes 9.0.6 (2026-09-03)

23 **Effecte hidden installed software exclusion** NEW 45

Adds Effecte advanced setting to exclude application installation records marked as hidden from Installed Software.

— Names the behaviour but not the setting key Axonius Release Notes 9.0.6 (2026-09-03)

24 **Custom Files adapter Last Seen override** NEW 42

Adds option to set the Last Seen value of Devices or Users to the current time in the Custom Files adapter.

— Single thin addition, minimal mechanism Axonius Release Notes 9.0.6 (2026-09-03)

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! The Cisco Firepower Management Center adapter no longer fetches ARP table data from firewall devices; the `Fetch ARP table from firewall devices` advanced setting has been removed. Access and NAT firewall rule assets no longer include a policy device name in their asset ID or firewall name.

! The CrowdStrike Falcon advanced setting `Enrich Configuration Assessment with Rule Name` is renamed to `Enrich Configuration Assessment with Rule Information`; any saved references to the old name must be updated.

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

defectdojo

Feedback ⓘ 1 RELEASE · 2026-09-01 BLOG ↗ RANK

Open-Source Unified Vulnerability Management, DevSecOps & ASPM

> DefectDojo Pro now lets teams export SBOM and VEX documents directly from Assets, via both a new REST API and an Asset-page UI panel, with support for CycloneDX 1.6, SPDX 2.3, and a combined SBOM-with-vulnerabilities (VDR) format.

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

01 **SBOM export endpoint for Assets** NEW 95

Adds `GET /api/v2/sbom/{asset_id}/` to export a CycloneDX 1.6 JSON SBOM for an Asset by default, with a `?spec=spdx` parameter to switch output to SPDX 2.3 JSON instead. A `?version=<release>` query parameter (e.g. `?version=5.2.0`) scopes the export to a specific Asset Version and returns 404 if that version does not exist.

Export a versioned SBOM in SPDX 2.3 JSON for a specific product release to satisfy a compliance or procurement request.

```
$ curl -H 'Authorization: Token <your_token>'
'https://<your_instance>/api/v2/sbom/<asset_id>/?
spec=spdx&version=5.2.0'
```

— Names endpoint, both formats, version param, and error behavior.

launch-20260901-e8cfa639

02 **VEX export endpoint for Assets** NEW 85

Adds `GET /api/v2/sbom/{asset_id}/vex/` to export a CycloneDX VEX document derived from the Asset's triage findings. Supports the same `?version=<release>` query parameter to scope the VEX output to a specific Asset Version, returning 404 if the version does not exist.

Retrieve a VEX document scoped to a specific release, reflecting per-version exploitability based on your team's triage and fixed_in records.

```
$ curl -H 'Authorization: Token <your_token>'
'https://<your_instance>/api/v2/sbom/<asset_id>/vex/?
version=5.2.0'
```

— Endpoint, derivation source, and version param are specified. launch-20260901-e8cfa639

03 **Export panel and VDR format on Asset page** NEW 60

Adds an Export panel to every Asset page in the DefectDojo Pro UI offering three export options: SBOM, VEX, and a new SBOM-with-vulnerabilities (VDR) format that embeds a VEX analysis block inside the CycloneDX SBOM inventory. The panel requires V3 Locations to be enabled.

— UI location and requirement given, but no exact navigation path.

launch-20260901-e8cfa639

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

Zscaler

Feedback ⓘ 1 RELEASE · 2026-09-04 BLOG ↗ RANK

Zscaler is a cloud-based security platform that inspects and filters internet traffic to protect against threats and enforce security policies.

> Zscaler launched two new AI-focused security capabilities for endpoints and identity, alongside a three-part CrowdStrike integration spanning adaptive access, SIEM telemetry, and SOAR-driven remediation.

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

01 **CrowdStrike SSF integration with Adaptive Access Engine** NEW 67

A new integration using the OpenID Shared Signals Framework (SSF) lets the CrowdStrike Falcon platform continuously share user-risk signals with Zscaler's Adaptive Access Engine (AAE), so access policies adjust dynamically in real time when suspicious endpoint behavior is detected.

— Names the protocol and engine but no setup steps included 2026-09-04-b2a6854a

02 **Endpoint AI Security Attack Chain Analysis** NEW 62

A new capability, powered by OpenAI GPT cyber models, evaluates an endpoint's full state — including local AI agents, browser extensions, packages, and system configurations — and constructs a realistic attack chain from initial lure to code execution, producing a prioritized remediation roadmap instead of a flat CVE list.

— Clear mechanism and inputs described, but no UI path or command given

2026-09-04-b2a6854a

THINNER COVERAGE BELOW

03 **Remediation actions from Charlotte Agentic SOAR** NEW 57

Analysts can trigger Zscaler enforcement actions and automated remediation directly from within the Charlotte Agentic SOAR interface, running natively inside the CrowdStrike Falcon platform with no middleware or separate infrastructure required.

— Names the SOAR product and native integration, gives a UI starting point

2026-09-04-b2a6854a

04 **AI Access Graph for identity risk** NEW 54

Maps human, service-account, and AI-agent identities to data objects and cloud endpoints, traces access paths, flags overprivileged or toxic permission combinations,

and ranks risks by business impact, blast radius, and resource confidentiality across multi-cloud environments.

— Mechanism explained well but no navigation or command to try it `2026-09-04-b2a6854a`

05 **Telemetry streaming into CrowdStrike Falcon Next-Gen SIEM**

NEW

43

Zscaler telemetry and AI-event metadata now stream directly into CrowdStrike Falcon Next-Gen SIEM, enabling unified cross-domain visibility and end-to-end investigation across user behavior and network traffic in a single console.

— Names the SIEM target but no configuration detail given `2026-09-04-b2a6854a`

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

ConductorOne

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

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

> ConductorOne shipped a major system log schema overhaul — new actor types, an API audience field, and four new event classes — alongside AI agent classifiers with an Observe mode, MCP resource governance, a guided MCP server registration flow, and a wave of role-mining, access-request, and findings-management improvements across four releases.

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

01 System log actor-type, audience, and event-class overhaul

90

BREAKING

System log events now distinguish administrator-tier actors via `actor.user.type_id` value `2` / `actor.user.type` value `"admin"` (non-admin users remain `type_id` `1` / `"user"`), and machine identities (connectors, managed connectors, functions, tunnels) now log as `type_id` `4` (shown as the standard Service account type) instead of the retired `type_id` `99` (Other), effective September 3, 2026. Events also gain an `actor.user.groups[]` array listing each actor's platform roles by display name with a stable `uid`, and a `metadata.correlation_uid` field linking the paired API Activity and Identity & Access events produced by a single privilege change. API Activity events (`class_uid` 6003) add an `unmapped.audience` field (`basic_user`, `admin_only`, `super_admin_only`, `machine_only`, or `unassigned`), a matching `audience=` value in `api.request.flags`, and new `class_name` / `category_name` caption fields. Four new Identity & Access event classes are emitted: `3001` (Account Change), `3004` (Entity Management), `3005` (User Access Management), and `3006` (Group Management). Existing queries filtering `type_id = 1` / `type = "user"` or `type_id = 99` must be updated, pipelines with fallthrough handlers must explicitly route the four new `class_uid` values, and most events are larger under the new schema, increasing volume-based ingest costs.

— Full breaking schema change with exact field names and migration guidance.

September 4, 2026 (2026-09-03)

02 Bulk request entitlement limit NEW

80

Admins can set a maximum number of entitlements a user may request at once in a single bulk request, from `Governance > Forms > Configure tenant-wide request settings`, with a range of 1–100 and a default of 10.

Cap the number of entitlements a user can request at once in a bulk request to reduce over-provisioning risk.

> 📍 In the ConductorOne console, go to Governance › Forms › Configure tenant-wide request settings and set the bulk request limit to a value between 1 and 100 (default is 10).

Set a tenant-wide bulk request limit so users cannot request more than 5 entitlements at once in a single bulk request.

> 📍 In the ConductorOne console, go to Governance › Forms › Configure tenant-wide request settings, then set `Max entitlements per bulk request` to 5 (valid range: 1–100, default: 10).

— Exact UI path, range, and default given with runnable steps.

September 4, 2026 (2026-09-03)

---

03 **AI agent classifiers with Observe mode** NEW — 65

New agent classifiers let admins write rules over private-data sensitivity, untrusted-content exposure, and exfiltration capability evaluated at call time, routing matches to a hook, human approval, or a block. An Observe mode logs what a rule would have caught without enforcing it, for safe rollout before enabling blocking.

— Mechanism and modes described but no exact config surface named.

September 4, 2026 (2026-09-03)

---

04 **Automation expression compilation change** BREAKING — 65

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

— Exact before/after and migration timing for existing automations.

September 4, 2026 (2026-09-03)

---

05 **Finding 'Owner' field renamed to 'Assignee'** BREAKING — 65

The `Owner` column, filter, and detail field on the Finding object is renamed `Assignee` across the UI, API, webhooks, and audit log; API, webhook, and SIEM consumers must update field and event-name references.

— Names exact surfaces affected across API, webhook, and audit log.

September 4, 2026 (2026-09-03)

---

06 **Session policy preview API endpoints** NEW — 60

Four new read-only API endpoints let admins preview which session policy applies to a given user — by direct assignment, group membership, or tenant default — and list every user a given policy covers, including users covered via group membership with the conferring group named.

— Endpoints described but no exact paths or methods given. September 4, 2026 (2026-09-03)

07 **MCP resource governance** NEW 60

A new Resources tab in MCP server management surfaces newly discovered static resources and URI templates for admin approval; each approved resource gets its own read entitlement, governed separately from tool and toolset access.

— Names the UI tab but no exact endpoint or config key. September 4, 2026 (2026-09-03)

08 **Expiring-access reminder notifications** NEW 60

ConductorOne now sends automated expiring-access reminder notifications to users at 30 days, 14 days, three days, one day, and one hour before a time-limited grant expires, with expiring access also surfaced in C1 digests.

— Exact reminder intervals given, no configuration control mentioned. product docs

THINNER COVERAGE BELOW

09 **Role mining threshold and enrollment approval routing**

IMPROVED 55

Role mining adds a configurable shared-access threshold (with a slider and histogram) to focus results on entitlements a cohort actually has in common, lets admins fine-tune the entitlement list before acting, and can optionally route automatic profile enrollments through an access request task for approval.

— Names the threshold and enrollment-routing mechanism, no exact config keys.

September 4, 2026 (2026-09-03)

10 **SSO silent, fresh, and passive authentication handling**

IMPROVED 55

SSO applications now honor OIDC silent and fresh authentication requests and SAML passive requests; requests that cannot be completed safely — such as SAML forced authentication without verifiable upstream evidence — now return an error instead of silently reusing an existing session.

— Clear before/after behavior but no config toggle named. September 4, 2026 (2026-09-03)

11 **Findings reprocessing** NEW 55

Findings can now be reprocessed against current transformation and routing rules — individually, in bulk, or from a finding's detail view — with the option to keep or reset

manual changes made to the finding.

— Describes trigger points and options but no API or flag named.

September 4, 2026 (2026-09-03)

12 **New 'Connector sync failing' finding type** NEW 55

A new Connector sync failing finding type is raised after two consecutive failed full syncs on a connector; it auto-resolves on the next successful sync and can be disabled per tenant.

— Exact trigger and resolution behavior, no config key for disabling given.

September 4, 2026 (2026-09-03)

13 **Guided MCP server registration flow** IMPROVED 50

Registering an MCP server now uses a guided step-by-step flow — covering server identity, hosting location, URL, access policy, tool discovery defaults, and authentication one question at a time — replacing the previous single multi-step form.

— Describes the flow's steps but not exact fields or validation.

September 4, 2026 (2026-09-03)

14 **Auto-created API credential on desktop device registration** NEW 50

Registering a new desktop device now auto-creates a full-access API credential, displayed on the device's registration success screen.

— Clear trigger and where the credential appears. September 4, 2026 (2026-09-03)

15 **Access request form duration and suspension visibility** IMPROVED 50

Access request forms now display an entitlement's duration limit up front — Indefinite is hidden when a max is set, and invalid existing durations are auto-adjusted — and flag when the target user or the holder of already granted access is suspended.

— Two form behaviors described, no field names given. September 4, 2026 (2026-09-03)

16 **Same-app entitlement bindings** NEW 50

The entitlement binding picker now shows entitlements from the same app, enabling same-app bindings such as Salesforce Admin -> Salesforce Editor.

— Concrete example given but no exact UI path. September 4, 2026 (2026-09-03)

17 **Owners picker 'All users / Owners' toggle** IMPROVED 50

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

— Names exact UI toggle and location. September 4, 2026 (2026-09-03)

---

18 **Access profile enrollments chart filtering fix** IMPROVED

50

The Access profile enrollments chart on the AI & MCP analytics tab now counts only enrollments in profiles that include at least one MCP tool or toolset.

— Exact chart and filter logic named, no broader context. September 4, 2026 (2026-09-03)

---

19 **External Slack account auto-linking removed** BREAKING

45

External Slack accounts, including Slack Connect members, can no longer be linked to a ConductorOne user account by email match; affected users now have notifications skipped with a warning instead of being silently matched.

— Clear behavior change but no remediation steps given. September 4, 2026 (2026-09-03)

---

20 **Manual deprovisioning fallback for unsupported revokes**

IMPROVED 40

Revokes on connectors that cannot deprovision a given entitlement now route to manual deprovisioning instead of being falsely closed as Revoked.

— Behavior change stated plainly, no configuration detail. product docs

---

21 **In-place provisioning step reordering** IMPROVED 40

Provisioning steps on an entitlement can now be reordered in place with move up/down controls, without removing and re-adding them.

— Simple UI mechanism described, minimal detail. September 4, 2026 (2026-09-03)

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! Effective September 3, 2026: `actor.user.type_id` `1` / `actor.user.type` `"user"` no longer covers administrator-tier actors — admins now log as `type_id` `2` / `type` `"admin"`. Queries filtering `type_id = 1` or `type = "user"` to capture all human activity must be updated to type_id IN (1, 2) or type IN (`user` , `admin`).

! Effective September 3, 2026: `actor.user.type_id` `99` (Other) is retired for machine identities; connectors, functions, and tunnels now log as `type_id` `4`. Automation filtering `type_id = 99` for machine identities must switch to `type_id = 4`.

- ! Privilege-changing operations now produce two events (one API Activity, one Identity & Access) instead of one — dashboards or metrics based on event volume may double-count unless scoped by `class_uid`.
- ! Four new `class_uid` values (`3001`, `3004`, `3005`, `3006`) are emitted; pipelines with a fallthrough or default handler that routes by `class_uid` will misroute these events unless they are handled explicitly.
- ! Most system log events are larger under the updated schema; volume-based ingest metering costs will increase.
- ! Automation expressions consisting of the bare workflow context, or that pass it to a function, no longer compile — expressions must reference the step and field directly. Already-running automations are unaffected until next edited and saved, at which point indirect-reference expressions must be rewritten to a static path.
- ! The `Owner` column, filter, and detail field on findings are renamed `Assignee`. API or webhook consumers of the Finding object and audit-log/SIEM pipelines must update to the new field and event names.
- ! Automation expressions that consist of the bare workflow context, or that pass it to a function, no longer compile — expressions must reference the step and field directly. Already-running automations are unaffected until next edited and saved, at which point indirect-reference expressions must be rewritten to a static path before saving.
- ! The `Owner` column, filter, and detail field on the Finding object (API, webhook, and audit log) are renamed to `Assignee` — consumers feeding findings via API, webhook, or a SIEM must update field and event-name references.

WAS THIS USEFUL? 👍 👎

Ping Identity

Feedback ⓘ 1 RELEASE · 2026-09-03 BLOG ↗ RANK

Read docs, explore use cases, learn best practices

> Ping Identity's documentation window centers on a large PingOneAIC/IGA release adding certification workflows, Friendly Captcha, and no-JS QR registration, alongside DaVinci's move to full per-flow content security policies and modernized accessible Forms rendering, plus early access for a PingOne Remote MCP Server and two breaking changes affecting ESV secrets and relationship creation.

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

01 ESV Google Secret Manager kid format change BREAKING

95

ESV secrets in Google Secret Manager now default to a unique name-and-version identifier as the JWK `kid`; installations relying on the legacy GSM-version-only `kid` must set `esv.am.secrets.gsm.stableid.version.only=true` to preserve prior behavior.

Preserve the legacy GSM JWK kid format after upgrading, to avoid breaking existing key references that depend on the version-only identifier.

```
$ esv.am.secrets.gsm.stableid.version.only=true
```

— Exact env var, default change, and runnable mitigation given. 02 Sep 2026 (2026-09-03)

02 Accessible PingOne Forms rendering IMPROVED

60

Improves PingOne Forms rendering with enhanced ARIA attribute usage, focus management, keyboard navigation, screen reader support, and error messaging.

— Lists concrete accessibility mechanisms with illustrative screenshots. product docs

03 No-JavaScript QR codes for MFA registration nodes NEW

60

Combined MFA Registration, OATH Registration, and Push Registration nodes now include an option to render QR codes without JavaScript.

— Names all three affected nodes and the new toggle behavior. 02 Sep 2026 (2026-09-03)

04 IGA role composition certification NEW

60

IGA role composition certification enables reviewers to certify role definitions, including attributes, glossary data, entitlements, applications, and membership rules.

— Names all certified components; lacks a review procedure. 02 Sep 2026 (2026-09-03)

THINNER COVERAGE BELOW

05 **Friendly Captcha support in v2 CAPTCHA node** NEW 55

Adds Friendly Captcha support to the `v2 CAPTCHA` node as a privacy-focused CAPTCHA provider alternative.

— Names the specific node; clear starting point to enable. 02 Sep 2026 (2026-09-03)

06 **PingOne Remote MCP Server (early access)** NEW 50

Introduces PingOne Remote MCP Server as an early access feature, opt-in via the PingOne admin console or the PingOne API.

— Names enablement paths but no config detail or limits. product docs

07 **Full per-flow custom content security policies in DaVinci** NEW 50

Adds custom content security policy (CSP) options, now generally available, allowing full CSP customization per flow.

— Describes GA scope but no exact config surface shown. product docs

08 **IGA identity profile certification** NEW 50

IGA identity profile certification enables reviewers to certify identity records — including external users and AI agents — rather than access alone.

— Explains scope shift to identity records but no workflow steps.

02 Sep 2026 (2026-09-03)

09 **Certification campaign and template administration** NEW 50

IGA now lets you delete certificate templates via the UI, and lets you change the campaign title and owner after a campaign is launched.

— Two named admin actions with a clear UI starting point. 02 Sep 2026 (2026-09-03)

10 **Role request form membership handling** IMPROVED 50

IGA role request forms display current role membership as read-only; each member addition or removal in the role lifecycle management screen is submitted as an individual grant or removal request.

— Describes new form behavior without exact screen path. 02 Sep 2026 (2026-09-03)

11 **Managed user update conflict handling** IMPROVED 50

Managed user updates that conflict with generated attribute values are now accepted and propagate to all associated workforce application accounts during queued synchronization.

– Explains before/after sync behavior but no config trigger. 02 Sep 2026 (2026-09-03)

12 **Stricter Advanced Identity Cloud relationship validation** 50

BREAKING

Advanced Identity Cloud now rejects relationship creation requests that reference a property not accepting the given object type, rather than silently routing through a different property.

– Explains behavior change but gives no remediation steps. 02 Sep 2026 (2026-09-03)

13 **Correlation rules for unmanaged applications** NEW 45

IGA correlation rules for unmanaged applications let administrators link aggregated accounts to identities during account aggregation.

– Explains purpose but not rule configuration details. 02 Sep 2026 (2026-09-03)

14 **IGA activity and notification monitoring GA** IMPROVED 40

IGA activity and notification monitoring is now generally available, with improved event type filtering and audit log presentation.

– States GA and improvements but no filter names or UI path. 02 Sep 2026 (2026-09-03)

15 **Approval tasks with workflow-variable expiration** NEW 25

Approval tasks can now be created when expiration is configured with a workflow variable.

– Single-sentence mention with no configuration example. 02 Sep 2026 (2026-09-03)

16 **IGA certification review views** NEW 20

IGA certification review views let reviewers examine identity-profile and role-composition items in dedicated task views.

– One-line description with no further mechanism given. 02 Sep 2026 (2026-09-03)

└──▷ ALSO FROM THESE RELEASES

└──▷ BREAKING ON UPGRADE

! ESV secrets in Google Secret Manager now default to a unique name-and-version identifier as the JWK `kid`; installations relying on the legacy GSM-version-only `kid` must set the `esv.am.secrets.gsm.stableid.version.only` environment variable to `true` to preserve prior behavior.

! Advanced Identity Cloud now rejects relationship creation requests that use a property not accepting the referenced object type; previously these were silently created via a different valid property.

WAS THIS USEFUL? 👍 👎

authentik

Feedback ⓘ 1 RELEASE · 2026-09-01 BLOG ↗ RANK

The authentication glue you need.

> authentik 2026.8 ships a wave of Enterprise access-governance features — privileged access management, agent accounts, scheduled user offboarding, and custom object attributes — alongside OAuth 2.0/RFC 8693 token exchange, dynamic client registration, a Rust-rewritten outpost, and full OpenID Certification, while making `AUTHENTIK_WEB__BASE_URL` a soon-required setting and changing how `hash_password` accepts input.

└──▷ **WHAT SHIPPED · 27 FEATURES** most completely described first ? what's the number?

01 Required base URL setting via AUTHENTIK_WEB__BASE_URL

90

BREAKING

Adds the `AUTHENTIK_WEB__BASE_URL` environment variable (also exposed as the Base URL setting under System > Settings and via API) to record the external URL of the authentik instance; the setting becomes required starting in 2026.11.

Set the required base URL for your instance via environment variable before the 2026.11 deadline, ensuring event links and redirects resolve correctly.

```
$ AUTHENTIK_WEB__BASE_URL=https://auth.example.com
```

— Names exact env var, setting path, and deadline.' launch-20260901-a8e8b0a6

02 OAuth 2.0 token exchange with RFC 8693 on-behalf-of support

NEW 90

Adds OAuth 2.0 token exchange, enabled per-provider under the Grant Types setting, letting applications trade a trusted token for an authentik access token representing the same user. Also adds RFC 8693 on-behalf-of (OBO) token exchange: clients supply `actor_token` and `actor_token_type` to receive a token carrying both the user and the actor via the `act` claim.

Enable OAuth 2.0 token exchange on a provider so a service can trade an upstream token for an authentik access token without forwarding the original credential.

📍 In the Admin UI, open Providers › <your provider> › Edit, locate the Grant Types setting, and enable Token Exchange. Then configure trusted providers or sources under the provider's JWT federation settings.

— Names setting and params; only UI steps given, not a full command.

launch-20260901-a8e8b0a6

03 **Privileged access management workspace (Enterprise)** NEW

75

New privileged access management (Enterprise) lets users request access to applications and entitlements from the UI; admins define request rules controlling requestors, approvers (users, groups, or policies), reviewer counts, and grant validity with automatic expiration and event-log tracking.

— Describes rules and mechanism but only a UI path, no exact navigation.

launch-20260901-a8e8b0a6

04 **Multi-account user switching** NEW

75

Multiple authentik accounts can stay signed in simultaneously in one browser and be switched via the account menu; enable by selecting a User switch flow for your brand, and policies control whether the switch requires a password, MFA, or a lighter check.

— Names the exact setting to enable, plus policy controls. launch-20260901-a8e8b0a6

05 **Custom object attributes for directory objects** NEW

75

New object attributes — custom text, number, and Boolean fields — are defined under `Directory > Object attributes`, with required/unique/regex-validation options, and are surfaced when editing users, groups, application entitlements, and device access groups, and enforced through the API.

— Names exact UI path and validation options. launch-20260901-a8e8b0a6

06 **hash_password no longer accepts positional password** BREAKING

75

The `hash_password` management command no longer accepts a positional password argument (to prevent shell-history exposure); run it without arguments for an interactive prompt or pipe via stdin, e.g. `echo "$PASSWORD" | docker compose run --rm server hash_password`.

Pipe a password securely into hash_password for automation without exposing it in shell history.

```
$ echo "$PASSWORD" | docker compose run --rm server hash_password
```

— Gives exact replacement command. launch-20260901-a8e8b0a6

07 **Agent service-account type (Enterprise)** NEW

65

New agent accounts (Enterprise) are a service-account type that acts on behalf of a parent user when calling the authentik API, with configurable policy inheritance, expiration rules, and audit events; users can optionally self-create agents from the UI.

— Explains mechanism, no exact config path given. launch-20260901-a8e8b0a6

08 **Scheduled user offboarding (Enterprise)** NEW 65

Administrators can schedule deactivation or deletion of a user account at a specific date and time, with optional concurrent session and token revocation, review/cancel capability, automatic retry on failure, and full event-log records.

— Describes behaviour and options but no exact UI/config path. launch-20260901-a8e8b0a6

09 **Self-hosted event map tiles (Enterprise)** NEW 60

The events map now ships a bundled basemap with no external requests by default, supporting air-gapped deployments; each brand can use the bundled map or point at a self-hosted tile server under the Map tiles setting.

— Names the setting, limited on further config detail. launch-20260901-a8e8b0a6

THINNER COVERAGE BELOW

10 **OAuth/OIDC dynamic client registration (Enterprise)** NEW 55

Applications can self-register via OAuth 2.0 / OpenID Connect DCR with admin-controlled policy bindings, grant type restrictions, scope mappings, and token validity limits.

— Explains controls but no config surface named. launch-20260901-a8e8b0a6

11 **40+ new application integration guides** NEW 55

Over 40 new application integration guides added, including Microsoft 365 via WS-Federation, Directus, Discourse, HubSpot, Infisical, n8n, NocoDB, Notion, and Veeam Backup & Replication, plus new source guides for GitLab and JumpCloud login.

— Names many specific integrations, but only doc links. launch-20260901-a8e8b0a6

12 **Nested group hierarchy sync for LDAP sources** NEW 50

Adds a Sync Group Parents option to LDAP sources to preserve nested group hierarchy when synchronizing from a directory.

— Names the setting but no further mechanism given. launch-20260901-a8e8b0a6

13 **Key-bound OpenID Connect ID token issuance** NEW 50

Providers can issue OpenID Connect ID tokens requiring the client to prove key possession, available for authorization code, device code, and refresh flows.

— Explains supported flows, no config key given. launch-20260901-a8e8b0a6

14 **SAML 1.1 assertions from WS-Federation providers** NEW 50

WS-Federation providers can now issue SAML 1.1 assertions, enabling integration with Microsoft 365 and Entra ID.

— Names integrations, no config steps. launch-20260901-a8e8b0a6

15 **JSON verification and Cap provider for Captcha stage** NEW 45

The `Captcha` stage now supports JSON verification requests and the self-hostable Cap CAPTCHA provider.

— Names stage and provider, no config detail given. launch-20260901-a8e8b0a6

16 **Expiration dates on policy, group, and user bindings** NEW 45

Policy, group, and user bindings can now carry an expiration date and time after which they no longer grant access or contribute a successful policy result.

— Clear behaviour, no exact UI/API path. launch-20260901-a8e8b0a6

17 **Direct connection alongside transaction-mode pooler** NEW 45

PostgreSQL transaction-mode connection-pooler support: a separate direct connection can be configured alongside the existing pooler settings for operations requiring a stable session.

— Names the mechanism but not the exact setting keys. launch-20260901-a8e8b0a6

18 **Server and proxy outpost rewritten in Rust** IMPROVED 45

The server and proxy outpost have been rewritten in Rust (replacing Go), with health checks for server and worker now running through the Rust entrypoint.

— Explains scope and change, no user action. launch-20260901-a8e8b0a6

19 **AUTHENTIK_POSTGRESQL__CONN_OPTIONS deprecated** DEPRECATED 45

`AUTHENTIK_POSTGRESQL__CONN_OPTIONS` and its replica equivalent are deprecated and will be removed in an upcoming version.

— Names exact env var, no replacement given yet. launch-20260901-a8e8b0a6

---

20 **System Tasks page now surfaces partial failures** BREAKING 45

Tasks that logged errors but previously finished as successful (e.g. a sync that failed for a single object) now show as errors or warnings on the System Tasks page; existing pre-upgrade task statuses remain until those tasks run again.

— Explains behaviour change and migration note. launch-20260901-a8e8b0a6

---

21 **SAML ForceAuthn requires fresh authentication** BREAKING 40

SAML authentication requests that set `ForceAuthn` now require fresh authentication.

— Names the flag and new behaviour, no migration detail. launch-20260901-a8e8b0a6

---

22 **Prevent duplicate device option removed from WebAuthn stage** DEPRECATED 40

The Prevent duplicate device option has been removed from the WebAuthn setup stage; it was disabled by default since 2026.5.4, so no action is needed on upgrade.

— States exact change and needed action (none). launch-20260901-a8e8b0a6

---

23 **AKQL JSON field matching for numeric and Boolean values** IMPROVED 35

AKQL queries against JSON fields now match numeric and Boolean values in addition to strings.

— Describes behaviour change, no query examples. launch-20260901-a8e8b0a6

---

24 **Compact list view for Application Dashboard** NEW 35

The Application Dashboard gains a compact list view that is persisted in the browser alongside the existing card grid.

— Names UI location, no further detail. launch-20260901-a8e8b0a6

---

25 **OpenID Certified across multiple OP and logout profiles** NEW 35

authentik is now officially OpenID Certified for Basic, Implicit, Hybrid, Config, and Form Post OP profiles and RP-Initiated, Front-Channel, and Back-Channel logout profiles.

— Certification fact only, nothing to act on. launch-20260901-a8e8b0a6

26 **Ed448 signing key support for OAuth providers** NEW

30

Adds Ed448 signing key support for OAuth providers.

— Bare capability name only. `launch-20260901-a8e8b0a6`

27 **GitLab compatibility mode for SCIM providers** NEW 30

SCIM providers gain a GitLab compatibility mode.

— Bare capability name only. `launch-20260901-a8e8b0a6`

└──▷ BREAKING ON UPGRADE

! The `hash_password` management command no longer accepts a positional password argument (to prevent shell-history exposure); run it without arguments for an interactive prompt or pipe via stdin: `echo "$PASSWORD" | docker compose run --rm server hash_password`.

! The `Prevent duplicate device` option has been removed from the WebAuthn setup stage (it was disabled by default since 2026.5.4); no action needed on upgrade.

! `AUTHENTIK_POSTGRESQL__CONN_OPTIONS` and its replica equivalent are deprecated and will be removed in an upcoming version.

! `AUTHENTIK_WEB__BASE_URL` becomes a required setting in 2026.11; configure it now under System > Settings to avoid a future hard requirement.

! Tasks that logged errors but previously finished as `successful` (e.g. a sync that failed for a single object) now show as errors or warnings on the System Tasks page; existing pre-upgrade task statuses remain until those tasks run again.

WAS THIS USEFUL? 👍 👎

CrowdStrike Falcon Identity Protection

Feedback

ⓘ 1 RELEASE BLOG ↗ RANK

CrowdStrike Falcon Identity Protection defends against identity-based attacks by monitoring and securing user identities across cloud and on-premises environments.

> CrowdStrike introduced an Agentic Identity Provider that issues AI agents cryptographic identities and brokers short-lived, least-privilege access, alongside extensions of just-in-time and zero-standing-privilege access to Salesforce, GitHub, endpoints, servers, private apps, and AWS environments using Microsoft Entra ID.

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

01 **Just-in-time access to private apps via Seraphic Enterprise Browser**

NEW 65

Falcon Seraphic Enterprise Browser now delivers just-in-time access to private apps and enterprise resources — including Linux workloads over SSH, Windows workloads over RDP, custom apps, and SaaS/cloud/on-premises resources — without requiring additional agents or browsers.

— Names protocols and delivery mechanism, giving a clear entry point. undated-d4eecdeb

02 **Agentic Identity Provider for AI agents** NEW 60

Falcon Next-Gen Identity Security adds an Agentic Identity Provider (Agentic IdP) that automatically registers AI agents in a single directory and issues each a cryptographically verifiable identity, replacing service accounts and long-lived credentials. Falcon Guardian discovers AI agents across the enterprise, identifies their owners, and links each agent to the human or workload it acts on behalf of to maintain end-to-end attribution, while Agentic IdP brokers short-lived, least-privilege access for registered agents instead of assigning them standing credentials.

— Explains mechanism and components but no concrete config or command shown.

undated-d4eecdeb

THINNER COVERAGE BELOW

03 **Privileged access extended to Salesforce, GitHub, endpoints and servers**

IMPROVED 50

Falcon Next-Gen Identity Security extends just-in-time privileged access to Salesforce and GitHub, and extends zero-standing-privilege access to endpoints and servers,

granting elevated rights only when a task requires them and revoking those rights when finished.

– Names the target surfaces but gives no setup or UI path. undated-d4eecdeb

04 AWS privileged access support for Microsoft Entra ID IMPROVED

50

Modern privileged access for AWS now extends to environments using Microsoft Entra ID, whereas previously announced support covered AWS through Okta.

– States before/after scope but no configuration steps given. undated-d4eecdeb

WAS THIS USEFUL? 👍 👎

◆ Public Key Infrastructure (PKI)

DigiCert CertCentral

Feedback ⓘ 1 RELEASE · 2026-09-01

BLOG ↗ RANK

DigiCert CertCentral is a centralized platform for managing SSL/TLS certificates, automating issuance, renewal, and deployment across infrastructure.

> DigiCert launched Continuous Validation, a new service that automates DNS-based domain control validation to keep domains issuance-ready without manual intervention.

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

01 Continuous Validation service for DNS-based DCV NEW

64

DigiCert Continuous Validation connects DigiCert Trust Lifecycle Manager to a customer's DNS environment through DigiCert UltraDNS to automate continuous DNS-based Domain Control Validation (DCV). It monitors domain validation status, automatically refreshes DNS records before validation expires so certificate issuance and renewal can proceed without manual DNS changes, and automatically removes dangling DNS records once validation completes.

– Mechanism and named components given, but no config/API surface or setup steps.

launch-20260901-10d28c98

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

MIND

Feedback ⓘ 1 RELEASE · 2026-09-01 BLOG ↗ RANK

MIND data security platform puts data loss prevention (DLP) and insider risk management (IRM) on autopilot - automatically identify, detect & prevent data leaks

> MIND shipped a Claude Connector that exposes its DLP/IRM data through an MCP server, letting security teams query open issues, policies, resource inventory, users and roles, and audit logs in natural language directly inside Claude — with both individual CLI setup and one-click organization-wide deployment.

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

01 **MIND MCP server for Claude** NEW 90

Launches the MIND MCP server at `https://mcp.mind.io`, enabling read-only natural-language queries against open issues, policies, resource inventory, users and roles, and audit logs directly inside Claude. Register it in Claude Code with `claude mcp add --transport http mind-mcp https://mcp.mind.io -s user` followed by `claude mcp login mind-mcp`, and inspect available MIND tools without leaving the terminal via the `/mcp` command by selecting `mind-mcp`. Because the server speaks standard Model Context Protocol, it also works with any MCP-capable client beyond Claude Desktop and claude.ai.

Register and authenticate the MIND MCP server globally in Claude Code so you can query DLP data from any project or session.

```
$ claude mcp add --transport http mind-mcp https://mcp.mind.io -s user
claude mcp login mind-mcp
```

— Exact CLI commands and server URL given, runnable as-is

The MIND Claude Connector: DLP answers …

02 **Organization-wide Claude Connector deployment** NEW 62

On Claude Team and Enterprise plans, a single Owner can add the connector once for the whole organization via Settings > Connectors > Add custom connector, setting name to `mind-mcp` and URL to `https://mcp.mind.io`, after which it becomes available to all members without individual setup.

Add the MIND connector for your whole Claude Team or Enterprise organization so every member gets access without individual setup.

> 📍 In Claude, go to Settings › Connectors › Add custom connector. Set the name to `mind-mcp` and the URL to `https://mcp.mind.io`. Click Continue, then Add, then Connect. Sign in to MIND when your browser opens.

— Exact UI path given but it's navigation, not a command

The MIND Claude Connector: DLP answers …

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Third-Party & Vendor Risk (TPRM)

Tenchi Security Zanshin

Feedback ⓘ 1 RELEASE · 2026-09-03

NOTES ↗ RANK

Meet Zanshin: The SaaS platform that connects companies with their supply chains, promotes transparency, and manages cybersecurity and privacy risks.

> Zanshin's September 2026 release centers on automated SAQ scoring with human-review safeguards, plus a new in-platform notifications center, expanded third-party reporting, richer organization profiles, and Zoom Workplace monitoring.

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

01 **Weighted SAQ scoring and auto-grading** NEW 80

Self-Assessment Questionnaires now support weighted scoring and auto-grading, with configurable severity levels (Informativo to Crítico) set per question and per answer. On submission, Zanshin issues automatic Accept / Reject / Request Clarification recommendations against defined risk thresholds.

Configure a SAQ with risk-weighted scoring and automatic Accept/Reject thresholds to speed up vendor assessment reviews.

> 📍 Go to SEGUIDAS › Questionários , open or create a questionnaire, assign severity weights (Informativo through Crítico) to individual questions, set per-answer score values, and define acceptance thresholds — Zanshin will auto-recommend Accept, Reject, or Request Clarification on submission.

— Names severity levels and outcome states with clear setup steps.

Novidades do Zanshin | Setembro de 2026

02 **In-platform Notifications Center** NEW 70

A new Notifications Center, accessed via a bell icon in the top-right, delivers clickable, action-oriented alerts scoped to the active Organization and filtered by RBAC permissions. Unread alerts persist for 30 days and read alerts are retained for 7 days.

— Concrete retention numbers and scoping, but only a UI location.

Novidades do Zanshin | Setembro de 2026

03 **Organization profile firmographics and contacts** IMPROVED 70

The Configurações menu is replaced by a Perfil hub (MINHA ORGANIZAÇÃO > Perfil > Detalhes) supporting firmographic data: multiple legal IDs (CNPJ etc.), employee count,

annual revenue, and NAICS sector codes, with address autocomplete and sector-code suggestions. It also supports multiple department-specific contacts (Security, Compliance, Legal, etc.) with individual names, emails, and phone numbers, replacing the single generic contact email.

— Enumerates every firmographic field and exact navigation path.

Novidades do Zanshin | Setembro de 2026

---

04 **Third-party report enhancements: language, gaps, compliance**

IMPROVED

65

Third-party reports can now be generated fully in Portuguese, removing language barriers with local suppliers. Reports also gain a dedicated Ambientes Ausentes (Missing Environments) section surfacing unmonitored scan targets, now display ISO 27001 and PCI DSS compliance coverage alongside existing frameworks, and include exact generation date/time plus an updated default file-naming convention for version control.

Review third-party supplier posture and share findings in Portuguese with local partners, including any unmonitored environment gaps and ISO 27001 / PCI DSS compliance status.

📍 Navigate to the third-party report for the target supplier, select Portuguese as the report language, and export — the report will include the Ambientes Ausentes section and ISO 27001 / PCI DSS compliance overview.

— Names all report additions with a generation workflow example.

Novidades do Zanshin | Setembro de 2026

---

05 **Zoom Workplace SaaS monitoring** NEW

60

Adds Zoom Workplace as a new supported SaaS environment type, available under Painel de Ambientes > SaaS, monitored using minimum-permission read-only security-configuration access.

Onboard Zoom Workplace for continuous security-configuration monitoring across your SaaS estate.

📍 In the platform, go to Painel de Ambientes › SaaS, locate Zoom Workplace, and follow the Zoom Workplace - Cadastro de Ambiente setup guide to grant minimum required permissions.

— Exact menu path and setup guide reference given.

Novidades do Zanshin | Setembro de 2026

THINNER COVERAGE BELOW

---

06 **SAQ reviewer interface** NEW

55

A new reviewer interface for SAQ assessments adds a side navigation panel, auto-advance to the next item, and manual override of automated scoring recommendations. It is accessible via `SEGUIDAS` > Questionários and `SEGUIDAS` > Avaliações.

— Exact menu path given but no worked example. Novidades do Zanshin | Setembro de 2026

---

07 **Partial-assessment mandatory review engine** NEW 50

A new partial-assessment engine flags free-text or evidence-file answers in SAQs as requiring mandatory human review before a final grade can be issued, preventing fully automated grading of ambiguous responses.

— Behavior described but no navigation or config given.

Novidades do Zanshin | Setembro de 2026

└──▷ **ALSO FROM THESE RELEASES**

.
.
.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

GitHub CLI

Feedback ⓘ 1 RELEASE · 2026-09-03 NOTES ↗ RANK

GitHub's official command line tool

> GitHub CLI v2.100.0 adds a per-host API gateway configuration and bundles the webhook extension as an official built-in, plus small improvements for coding-agent workflows.

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

01 **Per-host API gateway routing** NEW 88

A new `api_host` config key routes a GitHub host's API traffic through a custom gateway while leaving auth, Git remotes, and browser URLs on the original host. Set it with `gh config set api_host <gateway> --host <host>` and read it back with `gh config get api_host --host <host>`.

Route all GitHub API traffic through a corporate gateway — useful when your org requires API calls to pass through an inspection or compliance proxy.

```
$ gh config set api_host gh-gateway.example.com --host github.com
```

Confirm the gateway is configured correctly before relying on it in CI pipelines.

```
$ gh config get api_host --host github.com
```

— Exact config key and runnable commands given v2.100.0

THINNER COVERAGE BELOW

02 **Webhook extension bundled as built-in** NEW 35

The `webhook` extension is now an official built-in extension of GitHub CLI.

— Named but no usage detail given v2.100.0

03 **Full help output for coding agents** IMPROVED 30

When `gh` is invoked by a coding agent after a command misuse, it now prints full command help, improving agent-driven workflows.

— Behavior described but no invocation detail v2.100.0

WAS THIS USEFUL?  

joplin

Feedback ⓘ 1 RELEASE · 2026-08-31 BLOG ↗ RANK

Joplin - the privacy-focused note taking app with sync capabilities for Windows, macOS, Linux, Android and iOS.

> Joplin 3.7 is a major release built around new AI capabilities — an AI chat panel, semantic search, a built-in MCP server and an AI-focused plugin API — alongside a new whiteboards feature, notebook publishing to websites, Obsidian vault import, a table editor, and several smaller UI and performance improvements.

└──▷ **WHAT SHIPPED · 13 FEATURES** most completely described first ? what's the number?

01 **AI chat panel beside notes (Beta)** NEW 70

A new AI chat panel sits alongside the current note and can answer questions, summarise, edit, and read images. It works via Joplin Cloud AI with no API key required if already syncing with Joplin Cloud, or via a user-supplied OpenAI or Anthropic key, or a local model.

— Names backends and UI location but no config keys launch-20260831-5ad98b4f

02 **Semantic search across notes (Beta)** NEW 65

Semantic search, available in the sidebar and Go To Anything, matches notes by meaning rather than exact keywords, backed by a new background note embeddings indexer covering both titles and content.

— Mechanism and UI entry points given, no command shown launch-20260831-5ad98b4f

03 **Whiteboards for arranging notes** NEW 60

A new whiteboards feature on desktop lets users arrange notes, files, and free-form cards on an infinite canvas and connect them with labelled arrows; cards and groups can be coloured and files dragged onto the canvas.

— Behaviour well described, UI path is clear starting point launch-20260831-5ad98b4f

THINNER COVERAGE BELOW

04 **Built-in MCP server for notes** NEW 55

A new built-in MCP server lets external MCP-capable AI tools, such as Claude, read from and write to Joplin notes through a standard protocol.

— Describes purpose but no setup steps given launch-20260831-5ad98b4f

05 **Notebook publishing as a website** IMPROVED 55

Joplin Cloud users can now publish an entire notebook as a public website with preserved inter-note links, rather than only publishing individual notes as before.

— Before/after scope given, no exact publish steps launch-20260831-5ad98b4f

06 **Post-quantum cryptography for sync TLS** NEW 55

The desktop app now supports post-quantum cryptography (PQC) for TLS connections, protecting sync traffic against harvest-now-decrypt-later attacks.

— Names threat and protocol, no toggle or config given launch-20260831-5ad98b4f

07 **AI-focused plugin API (Beta)** NEW 50

A new plugin API (Beta) lets plugins hold conversations with a model, run semantic searches, and work with the note index directly.

— Capabilities named but no method names or examples launch-20260831-5ad98b4f

08 **Interactive table editor in Markdown editor** NEW 50

A new interactive table editor in the Markdown editor, on desktop and mobile, adds a context menu to add and delete rows and columns.

— UI mechanism named, screenshot shows menu launch-20260831-5ad98b4f

09 **Mobile notebook sort options** NEW 50

New notebook sort options on mobile let users sort alphabetically or by most-recently-updated, in either direction, configurable from the configuration screen.

— Options and UI location named clearly launch-20260831-5ad98b4f

10 **Settings search box** NEW 45

A new settings search box in the configuration screen lets users type to filter and surface matching settings across all sections.

— Clear UI location, no further mechanism detail launch-20260831-5ad98b4f

11 **Linux AppImage drops libfuse2 dependency** IMPROVED 45

The Linux AppImage no longer depends on the deprecated `libfuse2` library, enabling out-of-the-box installation on more distributions.

— Names dependency removed, no user action required launch-20260831-5ad98b4f

12 **Obsidian vault import** NEW 40

Adds support for importing an Obsidian vault on desktop and CLI.

— Bare statement of capability, no mechanism given launch-20260831-5ad98b4f

13 **Startup and crypto performance improvements** IMPROVED

40

Desktop startup is faster because plugin files that do not need processing are skipped at launch, and mobile encryption/decryption is faster after a refactor of the native crypto module.

— Two named mechanisms but automatic, nothing to configure `launch-20260831-5ad98b4f`

WAS THIS USEFUL? 👍 👎

INFRASTRUCTURE

◆ Internet Services

Cloudflare

Feedback ⓘ 2 RELEASES · 2026-08-31 → 2026-09-02 PRESS ↗

RANK

Connect, protect, and build everywhere.

> Cloudflare extended its Sandboxes platform to run Cursor Cloud Agents inside customer-controlled infrastructure and added a continuously self-retraining Adaptive Intelligence engine to Bot Management for catching evolving and low-and-slow bot attacks.

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

01 **Cursor Cloud Agents on Cloudflare Sandboxes** NEW 75

Cursor Cloud Agents can now run inside customer-controlled Cloudflare Sandbox environments via Cursor Self-Hosted Machines, keeping tool calls (terminal, filesystem, browser actions) inside the customer's Cloudflare account rather than on Cursor-managed infrastructure. Self-hosted worker pools act as named routing targets so new agent chats queue until a worker claims them, with pool orchestration to scale capacity on demand; a Cloud Agents API exposes machine status and pool routing for external systems. Connectivity is outbound-only — the Cursor worker opens a long-lived outbound HTTPS connection to Cursor's backend with no inbound connections required — and individual developers can connect a single worker via My Machines alongside enterprise team pool configurations. This extends Cloudflare Sandboxes' agent platform support alongside the previously announced Devin Outposts and Claude Managed Agents integrations.

— Names API, connectivity model and worker pools but no exact commands

launch-20260902-a34933be

02 **Adaptive Intelligence in Bot Management** IMPROVED 65

Cloudflare Bot Management gains Adaptive Intelligence, an ML detection engine that retrains continuously on live traffic to integrate new bot frameworks and bypass techniques in real time instead of waiting for scheduled updates. It adds multi-timeframe behavior analysis to catch low-and-slow attacks like slow credential stuffing and scraping, and combines browser-level session behavior signals from Cloudflare Precursor with global edge telemetry to evaluate automation beyond binary pass/fail tests; new security updates self-test against live traffic before deployment to verify accuracy and avoid false positives with zero downtime.

— Mechanism described in detail but no config or UI action given launch-20260831-ce3a6517

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 4, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue