THE CYBER TOOLCHAIN

NO. 094

# Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 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 160 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 38 tools

▾ // THE BRIEF

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

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. GitGuardian Self-Hosted now plants fake AWS credentials on endpoints so infostealer malware trips an

vim ? help

alarm the moment it harvests them. ScubaGear's `Invoke-SCuBADiff` compares two M365 assessment runs offline, turning tenant drift into a diff. And TruffleHog's `trufflehog analyze` tells you whether a found secret is still live and what it can reach.

DETECT

**Catch an infostealer at the moment it grabs credentials**

Decoy AWS keys seeded on endpoints fire only when something actually reads and uses them, which is a near-zero-false-positive signal for credential-harvesting malware. A dashboard card shows what fraction of the fleet is covered, so you can tell whether a silent week means safe or means unseeded.

GitGuardian Self-Hosted

RESPOND

**Know whether a leaked secret is actually dangerous before you page anyone**

`trufflehog analyze` checks a discovered secret for validity and enumerates what it can access, so triage starts with blast radius instead of a grep hit. New Jira, Bitbucket, Azure Repos and S3 sources also pull scanning into places secrets routinely land outside Git.

trufflehog

GOVERN

**Diff two M365 baseline assessments without a cloud round-trip**

`Invoke-SCuBADiff` compares two completed assessment runs offline, so configuration drift between last month and today is a report rather than a manual spreadsheet reconciliation. Useful for proving to an auditor that a control stayed in place, not just that it passed once.

ScubaGear

PROTECT

**Give an agent AWS access without handing it AWS keys**

nono proxies AWS calls with SigV4 signing so real keys never enter the sandboxed command's environment, closing the obvious exfiltration path when an agent goes off-script. Cloudflare made Zero Trust service-token authentication mandatory for new organizations, removing the weakest default from the service-to-service path.

nono · Cloudflare

Does **Opus 5** read better? 👍 👎

## OFFENSIVE SECURITY

◆ Exploitation & C2

# Bugcrowd Researcher Platform

Feedback ⓘ

changelog · Oct 4, 2026 CHANGELOG ↗ RANK

Bugcrowd Researcher Platform crowdsources security vulnerability discovery by connecting organizations with ethical hackers and security researchers worldwide.

> Bugcrowd Researcher Platform added a way for researchers to formally request withdrawal of a submitted response.

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

01 **Request a response withdrawal** NEW 35

Researchers can now use the Request a Response Withdrawal capability to formally request that a submitted response be withdrawn.

– Names the feature but no workflow or UI path detail changelog-20261004-1e68171c

WAS THIS USEFUL? 👍 👎

# Bishop Fox sliver

Feedback ⓘ v1.7.8 NOTES ↗ RANK

Adversary Emulation Framework

> Sliver v1.7.8 adds a service-naming flag for Windows implants, overhauls the credential-cracking dashboard, and exposes registry value types in read responses.

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

01 **Service name flag for implant generation** NEW 70

The `generate` command gains a `--service-name` flag to name Windows service implants at generation time.

— Names exact flag and command, minimal mechanism detail v1.7.8

02 **Real-time crack top dashboard** IMPROVED 60

`crack top` is redesigned as a real-time dashboard featuring a top panel and a benchmark cache policy.

— Names subcommand and two UI elements, no further mechanism v1.7.8

03 **RegistryType in registry read responses** NEW 60

Registry read responses now include a `RegistryType` field, exposing the value type alongside the registry data returned.

— Names exact field and response context, no usage example v1.7.8

THINNER COVERAGE BELOW

04 **Go toolchain updated to v1.27** IMPROVED 30

Implant and server builds now use Go v1.27 as the build toolchain.

— Bare version bump with no further detail v1.7.8

WAS THIS USEFUL? 👍 👎

◆ Hacking Hardware

## Hak5 WiFi Pineapple Pager

Feedback ⓘ 1.1.3-stable

NOTES ↗ RANK

A pocket sized WiFi Pineapple built for those on the go.

> WiFi Pineapple Pager 1.1.3 adds a WiFi Client Mode indicator and a new Quick Settings menu to the status bar interface.

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

01 **Quick Settings menu replaces Power Menu item** NEW 40

Adds a Quick Settings menu, replacing the first Power Menu item.

— Names exact UI location but little mechanism detail 1.1.3-stable

02 **WiFi Client Mode indicator in status bar** NEW 35

Adds a WiFi Client Mode indicator to the default status bar and the Network Status Bar.

— Names the UI surfaces but no mechanism 1.1.3-stable

WAS THIS USEFUL? 👍 👎

## Hak5 WiFi Pineapple

Feedback ⓘ sold out · Oct 3, 2026

STORE ↗

The leading rogue access point and WiFi pentest toolkit (Mark VII and Enterprise firmware).

Mark VII Basic (wifi-pineapple-mk7-basic) sold out at `shop.hak5.org` on 3 Oct 2026.

WAS THIS USEFUL? 👍 👎

## APPLICATION SECURITY

◆ Web Application Security

# Invicti

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> Invicti's Platform on-Demand release adds AI credit tracking and downloadable scanner logs for agentic pentests, improves time-based vulnerability confirmation accuracy, and introduces HTML report exports and scan log retention controls.

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

01 **Scanner log and agent trace download** NEW 55

Completed agentic pentest assessments now offer an option to download scanner logs and agent traces as a single compressed archive, intended for in-depth finding investigation or escalation to Invicti Support.

Download scanner logs and agent traces after an agentic pentest to investigate a finding in depth or escalate to Invicti Support.

> 📍 In the Invicti platform, open the completed assessment, then select the option to download scanner logs and agent traces as a single compressed archive.

– Clear action but no detail on archive format or size changelog-20261004-0d5b44c6

02 **HTML report download for assessments** NEW 50

Assessments can now be exported as a self-contained HTML report, openable in any browser, for sharing with stakeholders who lack platform access.

Share a self-contained assessment report with a stakeholder who does not have platform access.

> 📍 In the Invicti platform, open the assessment and choose the HTML report download option to produce a file openable in any browser.

– Clear UI action but no further format detail changelog-20261004-0d5b44c6

03 **AI Services Addendum reference in assessment dialog** IMPROVED 10

The assessment confirmation dialog now references the AI Services Addendum.

– Minimal wording change with no further context changelog-20261004-0d5b44c6

04 **Scan log retention controls** NEW 10

Invicti added scan log retention controls, as noted in the release summary, though no configuration details, defaults, or UI location were provided in the source material.

— Only named in summary, no supporting detail given changelog-20261004-0d5b44c6

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

# GitGuardian Self-Hosted

Feedback ⓘ

changelog · Oct 4, 2026 CHANGELOG ↗ RANK

GitGuardian Self-Hosted is an on-premise secret detection tool that scans repositories and prevents sensitive credentials from being committed.

> GitGuardian Self-Hosted adds honeytoken-based decoy AWS credentials to detect credential-harvesting malware on endpoints, with a new dashboard card to track fleet coverage.

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

01 **Honeytoken decoy AWS credentials for endpoint protection** NEW

72

Plants a decoy AWS credential in the file that credential-harvesting malware reads first, triggering an alert that names the compromised endpoint when the honeytoken is used. A new coverage card on the Endpoints dashboard shows the share of your fleet protected by the decoy credential feature. The feature requires Endpoint Protection, Honeytoken, and ClickHouse enabled on your instance.

Enable honeytoken-based AWS decoy planting for endpoint protection — navigate to the Endpoints dashboard to verify fleet coverage after enabling.

> 📍 In the Endpoints dashboard, open the coverage card to review the share of your fleet protected by the decoy AWS credential. Requires Endpoint Protection, Honeytoken, and ClickHouse enabled on your instance.

— Explains mechanism and dashboard location, but lacks exact config/API names.

changelog-20261004-815295c5

WAS THIS USEFUL? 👍 👎

# GitGuardian Detection Engine

Feedback ⓘ

changelog · Oct 4, 2026 CHANGELOG ↗ RANK

GitGuardian Detection Engine scans code repositories to identify and alert on exposed secrets, credentials, and sensitive data.

> GitGuardian expanded its detection engine with nine new secret detectors, a new analyzer for Cohere API keys, and a refined precedence rule for overlapping Base64 findings.

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

01 **Nine new secret detectors added** NEW 50

Adds detectors for Ory API keys, Kong Konnect personal access tokens, AppSignal API keys, PostHog OAuth access tokens, PostHog OAuth refresh tokens, Datadog service access tokens, NinzaSMS API keys, TypeSafe AI API keys, and the `mistralai_apikey_v2` detector for Mistral AI's new prefixed API key format.

— Names each detector but no scan setup or config detail changelog-20261004-709fc8a1

02 **Base64 Basic Auth precedence over generic entropy findings**

IMPROVED 40

Base64 Basic Authentication findings now take precedence over overlapping Base64 Generic High Entropy Secret findings, resolving duplicate or conflicting alerts on the same match.

— Explains behavior change but no config or scope detail changelog-20261004-709fc8a1

03 **New analyzer for Cohere API keys** NEW 23

Adds a new analyzer for Cohere API keys.

— Bare name, no detail on analyzer mechanism changelog-20261004-709fc8a1

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

# Veracode

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> Veracode's October update adds pipeline customization for Azure DevOps packaging, a mitigated-findings view in VS Code, team-level access controls for large Security Labs orgs, and a breaking overhaul of its Azure DevOps extension's import and scan tooling.

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

01 **predependency_command parameter in Azure DevOps Workflow** NEW

75

Azure DevOps Workflow Integration v2.4.4 adds a `predependency_command` parameter, letting pipelines run single-line or multiline commands before Veracode packages the project.

– Names exact parameter and version but no further mechanism detail

changelog-20261004-0b1c40da

02 **Azure DevOps Extension v4.0.0 Flaw Importer overhaul** BREAKING

70

Azure DevOps Extension v4.0.0 replaces Veracode Flaw Importer v3 with `VeracodeFlawImporter v4` and updates Upload and Scan to v4; existing pipelines on v3 must be manually migrated to v4 for both Azure DevOps Server and Azure DevOps (Cloud).

– Names exact components and migration requirement, lacks step-by-step guidance

changelog-20261004-0b1c40da

THINNER COVERAGE BELOW

03 **Mitigated Findings section in VS Code extension** NEW

55

Veracode Scan for VS Code v1.16.4 adds a Mitigated Findings section to the Flaws That Violate Policy view, surfacing findings with approved mitigations.

– Clear UI location named but no further workflow detail changelog-20261004-0b1c40da

04 **Team filtering for large orgs in Security Labs** IMPROVED

40

Organizations with more than 500 teams can now select which teams are available for use in Security Labs.

— States the capability but no mechanism or UI path changelog-20261004-0b1c40da

└──▷ **BREAKING ON UPGRADE**

! Azure DevOps Extension v4.0.0 deprecates Flaw Importer v3 and requires manually migrating existing pipelines from v3 to v4 for both Azure DevOps Server and Azure DevOps (Cloud).

---

WAS THIS USEFUL? 👍 👎

---

## Cloudsmith

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗

Cloudsmith is a fully-managed artifact management, software supply chain security, and software distribution platform.

Client log exports gain a `connected_repositories` field for download tracing; SCIM group provisioning is now GA on Ultra and Enterprise plans; CLI adds repo GPG key and access management.

Adds `connected_repositories` field to client log exports so you can trace a download back through every connected repository that served it.

Promotes SCIM group provisioning to general availability on Ultra and Enterprise plans, automatically syncing Cloudsmith team membership when users are added or removed from mapped IdP groups.

CLI v1.21.0–v1.26.0 adds commands to manage a repository's GPG key and access privileges from the terminal.

NEW INTEGRATION Nix package format support in Cloudsmith CLI

NEW INTEGRATION Cargo and pnpm credential helpers in Cloudsmith CLI

---

WAS THIS USEFUL? 👍 👎

## Semgrep

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> Semgrep rolled out SCIM-based user provisioning in public beta and surfaced Supply Chain security incidents directly on the Advisories page, alongside a redesigned Billing page.

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

01 **Supply Chain incidents on Advisories page** IMPROVED

45

The Advisories page now surfaces active or recent Supply Chain incidents at the top, and advisory Details pages link out to related incidents, dependencies, and blog posts.

— Describes the UI change but no config or API surface changelog-20261004-088a6a6d

02 **Redesigned Billing page with multi-product checkout** IMPROVED

20

Semgrep shipped a redesigned Billing page with multi-product checkout, per the release summary.

— Only mentioned in summary, no further detail given changelog-20261004-088a6a6d

WAS THIS USEFUL? 👍 👎

## CLOUD & CONTAINER SECURITY

◆ Container & Image Security

# Chainguard

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗

RANK

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

> Chainguard's FIPS Provider for OpenSSL v3.6 achieved FIPS 140-3 validation with post-quantum algorithm support, while Go and .NET Libraries entered an invite-only beta and 19 new container images shipped.

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

01 **FIPS 140-3 validation with post-quantum algorithms for OpenSSL v3.6**

NEW 80

The Chainguard FIPS Provider for OpenSSL v3.6 achieved FIPS 140-3 validation (Certificate #5523), supporting hybrid post-quantum key exchange for TLS that pairs classical key exchange with `ML-KEM` as an approved FIPS service, and includes standardized post-quantum algorithms `ML-KEM`, `ML-DSA`, and `SLH-DSA` alongside classical FIPS algorithms `AES`, `SHA-2`, `SHA-3`, `ECDSA`, and `RSA` in the validated module. Chainguard FIPS container images can opt in to the v3.6 module starting October 1, 2026.

— Names certificate, algorithms and opt-in date; lacks a runnable command

changelog-20261004-ee169bf3

02 **19 new container images added** NEW 60

Adds 19 new container images this week, including both standard and FIPS variants, among them `mcp-grafana-fips`, `kubernetes-pause-fips`, `chainguard-server-hypervisor-gcp`, `argocd-agent`, `victoriatraces`, `vault-secrets-webhook`, `ray`, `foundry`, `conftest`, `kured`, `keepalived`, `nix`, and `kates`.

— Names pullable images directly but no further mechanism detail

changelog-20261004-ee169bf3

THINNER COVERAGE BELOW

03 **SHA-1 dropped from FIPS v3.6 module** BREAKING 55

SHA-1 is not an approved algorithm in the newly validated OpenSSL v3.6 FIPS module; workloads using SHA-1 will break if they opt in to the module, which becomes available starting October 1, 2026.

— Clear before/after and date, but no migration guidance given

changelog-20261004-ee169bf3

04 **Tag-based Custom Assembly guides for Terraform and chainctl**

IMPROVED

50

Adds guides for managing tag-based Custom Assembly with the Chainguard Terraform provider and with `chainctl`, covering overlays and binding them to specific tags of a Custom Assembly repository.

— Names both tooling surfaces but is documentation, not a new capability

changelog-20261004-ee169bf3

05 **Invite-only beta for Go and .NET Libraries** NEW

40

Chainguard Libraries extends to the Go and .NET ecosystems through an invite-only beta, letting accepted organizations pull Go and .NET packages and evaluate them in existing development workflows.

— Describes scope but beta is invite-gated with no self-serve path

changelog-20261004-ee169bf3

└──▷ **BREAKING ON UPGRADE**

! SHA-1 is not an approved algorithm in the v3.6 FIPS module; workloads using SHA-1 will break if they opt in to the OpenSSL v3.6 module.

WAS THIS USEFUL? 👍 👎

# Aqua Security Trivy

Feedback ⓘ changelog · Oct 4, 2026

CHANGELOG ↗ RANK

Find vulnerabilities, misconfigurations, secrets, SBOM in containers, Kubernetes, code repositories, clouds and more

> Trivy adds a cryptographic asset scanner with CycloneDX output and ML-DSA support, alongside smaller improvements to Python vulnerability detection, lockfile parsing, licensing and package classification.

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

01 **Cryptographic asset scanning with CycloneDX output** NEW

70

Trivy adds a cryptographic asset model, parser, and analyzer that scans images and passes discovered assets to the scan report via the `image` command. Assets can be output in CycloneDX format and transferred in client/server mode, and the asset descriptions now support ML-DSA keys and signature algorithms.

– Names command and format but no flags or schema details changelog-20261004-4ed51b71

THINNER COVERAGE BELOW

02 **Package classification for julia, bottlerocket, and centos stream**

NEW

45

Trivy adds classification support for julia, bottlerocket, and centos stream packages.

– Names all three targets but no mechanism detail changelog-20261004-4ed51b71

03 **UNKNOWN severity for unparsable license names** IMPROVED

40

Trivy now reports unparsable license names with `UNKNOWN` severity.

– Names exact severity value but no further mechanism changelog-20261004-4ed51b71

04 **uv workspace lockfile parsing** NEW

35

Trivy now supports `uv` workspace lockfiles.

– Names the lockfile format but no further detail changelog-20261004-4ed51b71

05 **Disable config files with empty paths** IMPROVED

30

Trivy allows disabling configuration files with empty paths.

– States behaviour but no config key or flag named changelog-20261004-4ed51b71

## 06 Vulnerability detection for Echo-patched Python packages NEW

25

Trivy adds vulnerability detection for Echo-patched Python packages.

— Bare one-line addition with no mechanism `changelog-20261004-4ed51b71`

---

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

# Sysdig Secure

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗

RANK

Sysdig Secure is a container security platform providing runtime threat detection, forensics, and compliance monitoring for cloud-native environments.

> Sysdig Secure shipped AI-powered Threat Evaluation for ranking threats by likely maliciousness, a new Vulnerability Catalog for searching CVEs across tracked assets, and a preview of Supply Chain Findings.

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

01 **AI-powered Threat Evaluation on Threats page** NEW 80

Adds an Evaluation column to the Threats page (requires Secure AI entitlement) ranging from Malicious to Benign with Suspicious in between; the column is sortable and filterable, and a confidence level is shown in the Threats Detail panel.

Triage active threats quickly by surfacing the most likely malicious events first using AI-powered evaluation.

> 📍 In Sysdig Secure, go to Threats, click the Evaluation column header to sort descending (Malicious first), then use the Evaluation filter to narrow to Malicious and review confidence levels in the Threats Detail panel.

— Names exact column, values and entitlement, but not the underlying model

changelog-20261004-e0b53142

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

◆ CNAPP

# Plerion

Feedback ⓘ

Know which vulnerabilities are likely to be exploited: NOTES ↗ RANK

Plerion is a cloud security platform that discovers and manages vulnerabilities and misconfigurations across infrastructure.

> Plerion adds EPSS exploit-likelihood scoring across its vulnerability surfaces and overhauls its AgentCore memory accessibility check with more granular severity logic.

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

## 01 Revised AgentCore memory accessibility severity logic

75

BREAKING

The `[PLERION-AWS-1195]` AgentCore memory accessibility check now evaluates every read action an open policy allows, rating findings High when only an ARN is exposed, Medium when an ARN plus record or session ID is exposed, and Low when only user and session IDs are exposed. Existing findings previously rated High may be downgraded to Medium or Low on the next scan under this revised logic.

— Clear before/after mechanism with exact rule ID and rating logic.

Know which vulnerabilities are likely t…

## 02 EPSS exploit-likelihood scores for vulnerabilities NEW

68

Plerion now attaches an EPSS (Exploit Prediction Scoring System) score to every vulnerability, showing the probability of exploitation in the next 30 days as a percentage on the Vulnerabilities dashboard and code security issues. The score can be used to filter and sort vulnerabilities in the dashboard, set as a condition in workflow and exemption rule configurations, and is surfaced in alerts, tickets, CSV downloads, the customer API, and the CLI.

— Names all surfaces but no exact API/CLI command given.

Know which vulnerabilities are likely t…

└──▷ **BREAKING ON UPGRADE**

! Existing `[PLERION-AWS-1195]` AgentCore memory findings previously rated High may be downgraded to Medium or Low on the next scan under the revised severity logic.

WAS THIS USEFUL? 👍 👎

## DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

### CrowdStrike

Feedback ⓘ changelog · Oct 4, 2026 API ↗ RANK

CrowdStrike is a cybersecurity platform providing endpoint protection, threat intelligence, and incident response services.

> CrowdStrike's API expanded significantly in this window, adding new product surfaces for Seraphic enterprise browser security, a Scanning Orchestrator, Application Abuse Exclusions, and network scan detection/containment, alongside further operations for core host and incident workflows.

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

01 **Network Scan Detections and Containment APIs** NEW 50

New Network Scan Detections API operations let users review scan detections and report on scan results, and new Network Containment API operations allow managing network containment allowlists across scanned zones.

— Describes purpose of two related operation sets, no endpoint names 2026-10-04-b6de43bb

02 **Host and incident management API operations** NEW 30

16 new API operations were added spanning host management, detection investigation, incident response, and sensor tracking.

— Lists categories but no specific endpoints named 2026-10-04-22053f66

WAS THIS USEFUL? 👍 👎

# Huntress

Feedback

changelog · Oct 4, 2026

CHANGELOG ↗

RANK

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

> Huntress added five new Microsoft 365 hardening controls targeting inactive Entra accounts, shared mailboxes, spam, and Bookings, all schedulable for deployment.

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

01 **Five new Microsoft 365 hardening controls** NEW 66

Huntress added a set of schedulable Microsoft 365 hardening controls: an Entra control to block sign-in for member accounts inactive for 90 days, an Entra control to block sign-in for guest accounts inactive for 30 days, a control to block sign-in to shared mailboxes, an outbound spam policy control to set explicit sending limits and block senders, and a control to restrict Shared Bookings creation to selected users. All five are schedulable for deployment.

— Names specific thresholds and scopes but no exact UI path or API.

changelog-20261004-a8f72128

WAS THIS USEFUL?

# Corellium

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

Advice, answers, updates, and more from the Corellium Team

> Corellium expanded virtual device support to the latest iOS/iPadOS releases and brought on-premise deployments up to parity with the cloud.

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

01 **iOS/iPadOS virtual device support for new releases** NEW

50

Adds virtual device support for `iOS/iPadOS 26.5.2`, `iOS/iPadOS 26.6.0` RC1/GA, and `iOS/iPadOS 26.6.0` betas 2, 3, 4, and 5 (SA Falcon Premium subscribers only), plus `iOS/iPadOS 27.0.0` betas 1, 2, 3, and 4 (SA Falcon Premium subscribers only).

— Names exact OS versions and access tier but no setup steps changelog-20261004-ace7e4d2

02 **On-premise parity with 7.12.0 cloud release** IMPROVED

25

On-premise deployments are updated to reach feature parity with the 7.12.0 cloud release.

— States parity milestone without detailing which features caught up

changelog-20261004-ace7e4d2

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

# Tenzir

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

Tenzir is a data pipeline engine for security teams that collects, transforms, enriches, and routes telemetry.

> Tenzir's v6.19.0 release extended the ClickHouse integration with catch-all column support and Avro encoding, and improved Tenzir Test with structured CI reporting and selective warning suppression.

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

01 **ClickHouse catch-all columns and Avro encoding** IMPROVED

40

The ClickHouse integration now supports catch-all column support, allowing unmatched fields to be captured, and adds Avro encoding for data written to ClickHouse.

— Names two concrete additions but no config detail or mechanism

changelog-20261004-d8f431e7

WAS THIS USEFUL? 👍 👎

◆ SOAR

## Tines

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> Tines 43.5.0 expanded its AI model lineup with new GPT-6 and Claude options.

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

01 **New AI models: GPT-6 and Claude Opus 5.5** NEW 35

Tines 43.5.0 adds GPT-6 Astra, Sol, and Luna as available AI models, alongside Claude Opus 5.5.

.
.
.
.

— Names models but not how to select or configure them changelog-20261004-f882623f

WAS THIS USEFUL? 👍 👎

# EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

## runZero

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗

An asset discovery and inventory platform that identifies and maps all devices on networks without requiring agents.

Adds asset merge history view in the Manage menu on the asset details screen.

UPDATED SUPPORTED PLATFORM Fingerprint improvements for Cisco routers

UPDATED SUPPORTED PLATFORM Fingerprint improvements for Arista, Cisco, Echelon, Schneider Electric, Wind River, FreeNAS, and TrueNAS

UPDATED INTEGRATION Dragos integration performance improvement

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

# Cloudmersive

Feedback ⓘ

Cloudmersive Cloud Document AI API v2-13-0 Released (2026-10-03) BLOG ↗ RANK

Cloudmersive provides cloud-based APIs for document conversion, virus scanning, data validation, and content processing tasks.

> Cloudmersive shipped three incremental updates this window: new file format support for its Virus API, retry options for Document AI Managed Instance deployments, and expanded Advanced Virus Scan policy controls in the Reverse Proxy.

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

01 **DWF/DWFX format support in Private Cloud Virus API** NEW

40

Cloudmersive Private Cloud Virus API v11.10.28 adds support for scanning `.dwf` and `.dwfx` file formats.

— Names formats and version but no scan mechanism detail changelog-20261004-24b1248a

02 **Failure retry options for Document AI Managed Instance**

IMPROVED

25

Cloudmersive Cloud Document AI API v2-13-0 adds failure retry options for Managed Instance deployments.

— Bare description, no mechanism or config detail given

Cloudmersive Cloud Document AI API v2-1…

03 **Advanced Virus Scan policy options in Reverse Proxy** IMPROVED

25

Cloudmersive Reverse Proxy v4.16 adds additional policy configuration options for Advanced Virus Scan.

— Mentions feature area but no specific options named

Cloudmersive Reverse Proxy v4-16 (2026-…

WAS THIS USEFUL? 👍 👎

## IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

# Okta for AI Agents

Feedback ⓘ changelog · Oct 4, 2026

CHANGELOG ↗

Adds CIMD URL-based identity for AI agents, MCP server scope dialog, automatic manager-change reassignment for access requests, and a requester timeline view.

Adds CIMD (Client ID Metadata Document) support for AI agents, letting agents identify themselves with a URL instead of a static client ID.

Adds a separate dialog for custom MCP server scopes when adding scopes to an MCP server.

Adds automatic reassignment of pending manager tasks and manager questions to an employee's new manager on a manager change, preventing access-request blockage — works for both request conditions and request types.

Adds a requester timeline view in the Okta Access Request app, showing task status, individual approvals, and remaining tasks for requests built with access request conditions.

NEW INTEGRATION Atomicwork SAML OIN integration

NEW INTEGRATION Entrust IDV OIN integration

NEW INTEGRATION MongoDB Atlas SCIM 2.0 OIN integration

NEW INTEGRATION StitchOps OIDC OIN integration

NEW INTEGRATION Databricks AI agent import

WAS THIS USEFUL? 👍 👎

## iDenfy

Feedback

changelog · Oct 4, 2026

CHANGELOG ↗

Explore iDenfy documentation for identity verification (KYC), business verification (KYB), AML screening, fraud prevention, and more.

iDenfy Sprint 136 adds MCP for AI assistants, Age Estimation dashboard, Spanish business verification, and CPF date-of-birth collection.

### └──▷ HOW TO FIND IT

Let an AI assistant query iDenfy verification data via MCP — useful for building automated compliance review workflows in Claude or Claude Code.

> 📍 Connect Claude to your iDenfy account via the MCP integration, then use the consent screen to grant access only to the data areas (e.g. verification results) needed for your workflow.

Adds Age Estimation sessions to the dashboard, including session creation, filtering, and result details.

WAS THIS USEFUL? 👍 👎

# Keycloak

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

Keycloak - the open source identity and access management solution. Add single-sign-on and authentication to applications and secure services with minimum effort.

> Keycloak 26.8.0 adds OID4VCI and OID4VP verifiable-credential support, promotes multi-cluster v2 stateless mode and the SCIM API to supported while deprecating multi-cluster v1, and ships token delegation via Fine-Grained Admin Permissions, new Client Policy executors, and a wave of other preview/supported promotions; the Admin REST API separately deprecates four client-certificate endpoints.

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

## 01 Multi-cluster v2 stateless mode promoted to supported

95

BREAKING

Promotes multi-cluster v2 ( `--features=stateless` ) to supported, enabling multi-cluster deployments without an external Infinispan cluster by storing session data in the database; enable with `bin/kc.sh start --features=stateless` . Multi-cluster v1 (the `multi-site` feature) is deprecated and will be removed in a future major release — migrate to multi-cluster v2.

Enable multi-cluster v2 stateless mode so two Keycloak clusters share session state via the database, with no external Infinispan required.

```
$ bin/kc.sh start --features=stateless
```

— Runnable command and explicit deprecation/migration path changelog-20261004-91d2f674

## 02 OID4VCI credential issuance support NEW

90

Enables OID4VCI with `--features=oid4vc-vci` or `--features=preview` ; adds experimental `oid4vc-mdoc` format support, credential revocation on refresh token revocation, and an Application Initiated Action for in-session credential issuance.

— Exact feature flags, format, and mechanism named changelog-20261004-91d2f674

## 03 OID4VP verifier support for wallet presentations NEW

90

Adds `oid4vc-vp` experimental feature for OID4VP verifier support, enabling cross-device wallet credential presentations with `direct_post.jwt` encrypted response

mode and SD-JWT User Attribute and Session mappers. Enable with `bin/kc.sh start --features=oid4vc-vp`.

Enable OID4VP verifier support so users can authenticate by presenting verifiable credentials from their digital wallets.

```
$ bin/kc.sh start --features=oid4vc-vp
```

— Runnable command plus named mappers and response mode changelog-20261004-91d2f674

04 **Client Admin API v2 promoted to preview** NEW 85

Promotes Client Admin API v2 to preview, enabled with `--features=client-admin-api:v2` or `--features=preview`, with a Java client, auto-generated JavaScript client, CLI, and Operator `KeycloakClient` custom resources.

— Exact flag and client tooling surfaces named changelog-20261004-91d2f674

05 **Token delegation scopes via Fine-Grained Admin Permissions**

NEW 80

Auto-creates `delegation:user` and `delegation:client` client scopes as Optional scopes in all realms, with delegation authorization controlled via Fine-Grained Admin Permissions V2 `delegate` and `delegate-members` scopes.

— Exact scope names given, no setup command shown changelog-20261004-91d2f674

06 **New Client Policy executors for node validation and protocol mappers**

NEW 80

Adds `secure-client-node-hostname` client policy executor to validate cluster node hostnames against admin-configured regex patterns on the `/clients-managements/register-node` endpoint, preventing SSRF. Adds `allowed-protocol-mappers` executor to Client Policies to restrict protocol mapper types creatable via Admin REST API protocol mapper endpoints.

— Both executors and the endpoint named verbatim changelog-20261004-91d2f674

07 **Impersonation details in token lifecycle events** IMPROVED 75

Enriches `CODE_TO_TOKEN`, `REFRESH_TOKEN`, and other token lifecycle events with `impersonator` and `impersonator_id` details, and includes a non-disableable `act` claim in access and ID tokens for impersonation sessions.

— Named event types and claim, no config step shown changelog-20261004-91d2f674

08 **invite-user workflow step** NEW 70

Adds `invite-user` workflow step that automatically sends an action-token email when a user is created, with configurable required actions, client, and redirect URI.

– Step name and configurable fields given, no config path changelog-20261004-91d2f674

09 **SCIM API promoted to supported** IMPROVED 60

Promotes SCIM API to supported, adding multivalued user attributes, User Profile permissions, Fine-Grained Admin Permissions in search filters, and improved performance for large user bases.

– Named capabilities but no endpoint or command given changelog-20261004-91d2f674

10 **Account enable/disable RISC events via SSF** NEW 60

Emits `account-disabled` and `account-enabled` RISC event types from the experimental Shared Signals Framework (SSF) when a user is enabled or disabled.

– Named event types, no setup instructions given changelog-20261004-91d2f674

THINNER COVERAGE BELOW

11 **Client Secret Rotation promoted to supported** IMPROVED 55

Promotes Client Secret Rotation to supported, allowing confidential clients to hold up to two concurrently active secrets for zero-downtime rotation via client policies.

– Mechanism described, no exact policy config named changelog-20261004-91d2f674

12 **Parameterized scopes promoted to preview** NEW 55

Promotes Parameterized scopes (formerly dynamic scopes) to preview, allowing clients to pass a parameter value with the scope name in OAuth 2.0 authorization requests.

– Mechanism described, no enabling flag given changelog-20261004-91d2f674

13 **BCFKS truststore format in FIPS mode** IMPROVED 40

Generated system truststore uses BCFKS format in strict FIPS mode.

– Named format and mode, no config steps given changelog-20261004-91d2f674

14 **Encrypted PEM file support for TLS** NEW 35

Adds support for encrypted PEM files for TLS certificate and private key configuration.

– Thin one-line description, no config key shown changelog-20261004-91d2f674

15 **Non-blocking database index creation** IMPROVED 35

Adds automatic non-blocking index creation for large database tables.

– Behaviour named, no trigger or config given changelog-20261004-91d2f674

16 **Login failures stored in database** IMPROVED 30

Stores login failures in the database instead of in-memory.

– Bare before/after statement, no mechanism detail changelog-20261004-91d2f674

17 **CLI options for cluster and node name** NEW 30

Adds first-class CLI options for cluster and node name.

– Names the capability, not the actual flag names changelog-20261004-91d2f674

18 **Experimental Helm Chart Operator install** NEW 25

Adds experimental Helm Chart Operator install support.

– Bare name only, no chart path or command changelog-20261004-91d2f674

19 **Shared identity providers across organizations** NEW 25

Adds shared identity providers across organizations.

– Bare feature statement with no mechanism changelog-20261004-91d2f674

20 **Experimental Vert.x-based outbound HTTP client** NEW 20

Adds experimental Vert.x-based outbound HTTP client.

– Bare name only, no enabling flag or scope changelog-20261004-91d2f674

21 **Redesigned identity provider login buttons** IMPROVED 15

Redesigns identity provider buttons on the login page.

– Cosmetic change noted with no further detail changelog-20261004-91d2f674

└──▷ **BREAKING ON UPGRADE**

! Deprecated endpoint POST `/admin` /realms/{realm} `/clients` /{client-uuid} `/certificates` /{attr} `/download` (still works)

! Deprecated endpoint POST `/admin` /realms/{realm} `/clients` /{client-uuid} `/certificates` /{attr} `/generate` (still works)

! Deprecated endpoint POST `/admin` /realms/{realm} `/clients` /{client-uuid} `/certificates` /{attr} `/generate-and-download` (still works)

! Deprecated endpoint POST `/admin` /realms/{realm} `/clients` /{client-uuid} `/certificates` /{attr} `/upload` (still works)

! Multi-cluster v1 (the `multi-site` feature) is deprecated and will be removed in a future major release; migrate to multi-cluster v2 using `--features=stateless`.

WAS THIS USEFUL?  

# Didit

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> Didit's latest release focuses on white-label wallet sign-in branding, deeper database-lookup controls, stricter liveness and device-spoof detection, an expanded Copilot, and sandbox/currency improvements to Transaction Monitoring, alongside a webhook signature header deprecation.

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

01 **Sandbox labeling and currency support in Transaction Monitoring**

NEW 88

Transaction Monitoring now tags transactions evaluated on sandbox applications with a sandbox environment label, and an expanded currency picker lists every circulating currency with per-currency decimal formatting applied in transaction PDFs. Sandbox AML scenarios can be simulated directly via the API, e.g. `POST https://api.didit.me/v3/aml/` with `"sandbox_scenario": "hit"`, to test alert-handling logic without involving a real end-user session.

Simulate an AML hit in sandbox to test your alert-handling logic without involving a real end-user session.

```
$ curl -X POST https://api.didit.me/v3/aml/ \
  -H 'Authorization: Bearer <token>' \
  -H 'Content-Type: application/json' \
  -d '{"vendor_data": "test-user-42", "sandbox_scenario": "hit"}'
```

— Includes runnable sandbox API call plus concrete feature names

changelog-20261004-84557804

02 **Database lookup source selection and retry control** IMPROVED

70

Database lookups now support per-country source selection when more than one lookup source is available, a configurable retry control (one to five attempts, default one, counting only attempts the source actually answered), and a detailed per-field match breakdown showing what the user provided, what the source held, whether it matched, plus source-error details.

— Names mechanism and defaults but no exact config path changelog-20261004-84557804

03 **Copilot admin actions and conversation controls** NEW

65

Copilot can now switch organization or application, rename applications, duplicate/rename/archive/link workflows, open member/role/webhook/list dialogs, block a user, and download a session PDF; it also gains reply-language selection, Word and plain-text file attachment, and full conversation-history deletion.

— Lists many named actions but no command or endpoint changelog-20261004-84557804

04 **Liveness decline and device-spoof detection** IMPROVED

60

Liveness video analysis can now decline a session outright (not only report) on non-live recordings, and emulated/virtualized device detection during liveness capture is now surfaced as an actionable risk signal.

— Describes behaviour change but not configuration path changelog-20261004-84557804

05 **Webhook signature header deprecation** DEPRECATED

60

`X-Signature-Simple` is deprecated — webhooks should now be verified using `X-Signature-V2` instead.

— Names exact headers but no migration timeline given changelog-20261004-84557804

THINNER COVERAGE BELOW

06 **Self-service ticket closure in support console** NEW

53

The support console adds drag-and-drop attachment upload and self-service ticket closure, with reply-to-reopen.

— Clear UI capability but no navigation path given changelog-20261004-84557804

07 **White-label wallet sign-in pages** NEW

50

Wallet sign-in pages now support white-label branding, with Smart-ID and Mobile-ID running inside the same verification design.

— Names integrations but no setup detail given changelog-20261004-84557804

08 **Session timeline for workflow decisions** NEW

45

Workflow sessions now display a session timeline showing each branch decision and terminal status node.

— States what it shows but no mechanism or location detail changelog-20261004-84557804

└──▷ **BREAKING ON UPGRADE**

! `X-Signature-Simple` is deprecated — verify webhooks with `X-Signature-V2` instead.

WAS THIS USEFUL?  

## Clerk

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

Clerk is an authentication and user-management platform that provides pre-built UI components, APIs, and SDKs for adding sign-up, sign-in, and identity features to applications.

> Clerk shipped self-serve Directory Sync inside `<OrganizationProfile />` for enterprise SCIM provisioning, plus an SSO bypass allowlist letting users sign in via one-time email code when an enterprise SSO connection fails.

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

### 01 Self-serve Directory Sync in OrganizationProfile NEW

91

Adds a `org:sys_entconns:manage` permission-gated self-serve Directory Sync wizard inside the Security tab of `<OrganizationProfile />`, supporting Okta Workforce, Microsoft Entra ID, Google Workspace, and custom SAML/OIDC connections; admins get a generated SCIM endpoint URL and bearer token without needing Clerk Dashboard access. Google Workspace sync is configured via the Google Admin SDK by uploading a service account key and Workspace admin email inside the wizard, and a connection can be paused, resumed, or removed from within `<OrganizationProfile />` after setup. The feature is exposed by enabling the Allow this organization to set up enterprise SSO and Directory Sync toggle under Organization permissions in the Clerk Dashboard, which surfaces the section wherever `<OrganizationProfile />` or `<OrganizationSwitcher />` renders; Dashboard-side custom attribute mapping and role mapping (off by default) remain available alongside dashboard-managed directories.

Enable self-serve Directory Sync for an organization so its admin can configure SCIM provisioning without Clerk Dashboard access.

> 📍 In the Clerk Dashboard: select an Organization › open its Settings › under Organization permissions, turn on 'Allow this organization to set up enterprise SSO and Directory Sync'. The Directory Sync section then appears in the Security tab of <OrganizationProfile /> wherever it renders in your app.

— Names permission, toggle, providers, and setup flow with exact steps

changelog-20261004-38454fea

### 02 SSO bypass allowlist for broken connections NEW

77

Adds SSO bypass, a per-connection allowlist letting designated users sign in with a one-time email code when an enterprise SSO connection is broken or unavailable, surfaced via a 'Can't use SSO?' link in `<SignIn />`. A new `org:sys_entconns_sso_bypass:manage` system permission, included in the default

Admin role, lets Organization members manage the allowlist from `<OrganizationProfile />`, and each bypass sign-in logs a `sign_in.sso_bypass.succeeded` audit event.

— Names permission and audit event but no setup steps shown `changelog-20261004-38454fea`

---

WAS THIS USEFUL? 👍 👎

# Nudge Security

Feedback ⓘ changelog · Oct 4, 2026

CHANGELOG ↗ RANK

Nudge Security is a SaaS security platform that discovers shadow IT assets, manages identity governance, and hardens security posture.

> Nudge Security introduced two AI agents under Automations > AI Agents that automate remediation of OAuth grant risk and browser extension risk, each with human-in-the-loop oversight.

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

01 **OAuth Grant Risk Analyst AI agent** NEW 70

Accessible via `Automations > AI Agents`, this agent reviews new OAuth grants as they are discovered, automatically revokes overly permissive or high-risk grants, or nudges the OAuth grantor to remove access, with human-in-the-loop oversight.

Enable the OAuth Grant Risk Analyst to automatically revoke high-risk OAuth grants as Nudge Security discovers them, reducing manual triage.

> 📍 In the Nudge Security console, go to Automations › AI Agents, select OAuth Grant Risk Analyst, configure your revocation and nudge preferences, and activate the agent.

— Names mechanism and nav path but no config/API detail. changelog-20261004-599b0358

02 **Browser Extension Risk Analyst AI agent** NEW 70

Accessible via `Automations > AI Agents`, this agent inspects browser extension artifacts and metadata to flag malicious, compromised, or misrepresented extensions, and orchestrates disable and uninstall workflows.

Deploy the Browser Extension Risk Analyst to continuously inspect employee-installed extensions and trigger disable/uninstall workflows for flagged ones.

> 📍 In the Nudge Security console, go to Automations › AI Agents, select Browser Extension Risk Analyst, set your risk thresholds and remediation actions, and activate the agent.

— Describes inspection and remediation flow with nav path, no thresholds specified.

changelog-20261004-599b0358

WAS THIS USEFUL? 👍 👎

## JumpCloud

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> JumpCloud's September 2026 release adds an MCP Server letting users connect AI clients to the User Portal, Custom Risk Policies for logins across Admin Portal, User Portal, device and SSO surfaces, Apple MDM App Settings Privacy controls, asset visibility and acknowledgement, a custom banned password list, automatic device registration via JumpCloud Go, and User Portal application folders.

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

01 **MCP Server for Users** NEW 80

Adds JumpCloud MCP Server for Users, letting users connect AI clients to User Portal capabilities over OAuth; admins toggle it on and can configure automatic session expiration or manually revoke sessions, and users manage their own sessions under `JumpCloud MCP` in the User Portal.

Turn on the MCP Server for Users so staff can perform User Portal tasks directly from AI clients without switching tools.

> 📍 In the Admin Portal, navigate to the MCP Server for Users settings page and toggle on MCP Server for Users. To cap session lifetime, configure the automatic expiration window. Users can then view or revoke their own active sessions under JumpCloud MCP in the User Portal.

— Clear toggle path and session management location named. changelog-20261004-031e32d5

02 **App Settings Privacy policies for Apple MDM** NEW 75

Adds App Settings Privacy policies for Apple MDM: a User Level macOS policy (supervised Macs running macOS 27+, assignable to users or user groups, covering Accessibility, Bluetooth, Camera, Dictation, Local Network, Location, and Microphone) and a Device Level iOS/iPadOS policy (supervised iPhones and iPads running iOS 27+ or iPadOS 27+, assignable to devices or device groups, covering Bluetooth, Camera, Dictation, Local Network, Location, Location Accuracy, and Microphone).

— Names exact platforms, OS versions and privacy categories covered.

changelog-20261004-031e32d5

03 **Asset visibility and acknowledgement in Device Management**

NEW 75

Enables Asset Visibility and Asset Acknowledgement via `Device Management > Asset Management > Settings and Fields > General Settings` so end users see assigned assets in the User Portal and admins can request acknowledgement recorded in Asset History.

Enable asset visibility and acknowledgement prompts so users see IT-assigned assets and admins get a recorded response on every assignment.

> 📍 In the Admin Portal, go to Device Management › Asset Management › Settings and Fields › General Settings. In the User Portal section, enable Asset Visibility and Asset Acknowledgement.

— Exact UI path given with recorded acknowledgement mechanism.

changelog-20261004-031e32d5

---

04 **Custom Risk Policies for logins** NEW 65

Adds Custom Risk Policies for Admin Portal, User Portal, device, and SSO application logins, allowing admins to select risk factors, adjust score contributions, and set policy precedence per user group or SSO application, with a Default Policy covering unmatched logins.

— Mechanism described but no exact UI path or config key. changelog-20261004-031e32d5

---

05 **User Portal Folders for applications** NEW 65

Adds User Portal Folders so end users can organize assigned applications into private personal folders from the Folders tab on the All Applications page.

— Exact UI tab and page named for navigation. changelog-20261004-031e32d5

---

06 **JumpCloud Go automatic device registration** NEW 60

Adds JumpCloud Go automatic device registration for managed Windows, macOS, and Linux devices; admins control eligibility via device exclusion groups and can fall back to manual registration.

— Exclusion groups and fallback named but no exact config path.

changelog-20261004-031e32d5

└──▷ **ALSO FROM THESE RELEASES**

---

WAS THIS USEFUL? 👍 👎

# Ping Identity

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗

RANK

Read docs, explore use cases, learn best practices

> Ping Identity's Advanced Identity Cloud release added configurable email providers with test-send support, a SAML metadata signature-verification bypass, v2.0 Decision nodes for LDAP and Identity Store, Android EC key attestation, and a rename of ThreatMetrix nodes to LexisNexis DDP nodes alongside several smaller admin console and journey-canvas usability additions.

└──▷ **WHAT SHIPPED · 14 FEATURES** most completely described first ? what's the number?

01 **Configurable email provider with test send** NEW 73

Adds support for configuring Microsoft Entra ID or custom SMTP email providers in the Advanced Identity Cloud admin console, with the ability to send test emails to verify delivery before relying on them for production identity journeys.

Configure a custom SMTP email provider and validate it works before relying on it for production identity journeys.

📍 In the Advanced Identity Cloud admin console, go to Email Provider settings, select Custom SMTP or Microsoft Entra ID, enter your provider credentials, then click Send Test Email to verify delivery.

— Names both providers and exact UI steps with test-send mechanism

changelog-20261004-42bd0c0b

02 **LexisNexis DDP node rename and configuration updates** BREAKING 65

Renames ThreatMetrix nodes to LexisNexis Dynamic Decision Platform (DDP) nodes; adds a configuration option to the LexisNexis DDP Profiler node to inject scripts in the `head` element or in an iframe; and updates LexisNexis InstantID Question and Answer (IIDQA) nodes to store decision API responses in shared state.

— Names rename, injection option and shared-state change, but no migration steps

changelog-20261004-42bd0c0b

03 **Skip SAML metadata signature verification** NEW 63

Adds an option to skip XML signature verification when importing remote SAML 2.0 provider metadata, found under Federation > Remote Entity Providers when importing a

provider metadata URL.

Skip XML signature verification when importing a remote SAML 2.0 metadata document from a provider that does not sign its metadata.

> 📍 In the Advanced Identity Cloud admin console, go to Federation › Remote Entity Providers, import a SAML 2.0 provider metadata URL, and enable the option to skip XML signature verification before saving.

— Exact navigation path and trigger condition given `changelog-20261004-42bd0c0b`

04 **Journey canvas pan and multi-node selection** NEW 60

Adds pan support for journey canvases by holding the space bar and dragging with the left mouse button, and multi-node selection by holding Shift and clicking each node.

— Exact key/mouse combinations make it immediately usable `changelog-20261004-42bd0c0b`

THINNER COVERAGE BELOW

05 **Telephone number user property format** NEW 55

Adds telephone number as a user property format, with optional server-side validation and separate country code and phone number fields in hosted pages and the admin console.

— Describes validation and field structure, no config key named `changelog-20261004-42bd0c0b`

06 **EC key attestation for Android device binding** NEW 50

Adds EC key attestation support for Android device binding, enabling compatibility with newer Google hardware attestation root certificates.

— Explains compatibility benefit, no setup steps given `changelog-20261004-42bd0c0b`

07 **LDAP and Identity Store Decision nodes v2.0** IMPROVED 40

Adds v2.0 of the LDAP Decision node and the Identity Store Decision node with unspecified improvements over prior versions.

— Names versions and nodes but not what improved `changelog-20261004-42bd0c0b`

08 **Multi-value custom node properties** NEW 40

Adds the ability to select multiple values from predefined options when configuring custom node properties in the node designer.

— Names the designer surface but no steps `changelog-20261004-42bd0c0b`

09 **Next-generation scripting engine as default** IMPROVED

40

Makes the next-generation scripting engine the default and recommended option when creating scripts in the Advanced Identity Cloud admin console.

– States new default, no behavioural detail given changelog-20261004-42bd0c0b

10 **reCAPTCHA Enterprise node misconfiguration logging** IMPROVED

40

Adds logging of errors in the reCAPTCHA Enterprise node when its Google project, site key, or API key secret is misconfigured.

– Names the three misconfigurable fields, no log location given

changelog-20261004-42bd0c0b

11 **Reconciliation target phase selection** NEW

40

Adds `runTargetPhase` selection in the Advanced Identity Cloud admin console when running reconciliations.

– Names exact config option but no usage detail changelog-20261004-42bd0c0b

12 **Navigation profiles for hosted account pages** NEW

35

Adds navigation profiles to customize the hosted account pages navigation menu for different groups of users.

– States purpose, no mechanism or config detail changelog-20261004-42bd0c0b

13 **Backchannel transaction subject retention** IMPROVED

35

Backchannel transactions now record the authenticated subject on completion even when no session is created, preserving a subject declared before authentication.

– Explains behaviour change but no config or API surface changelog-20261004-42bd0c0b

14 **Search and sort for AI agent identities** NEW

30

Adds search and sort capabilities for the list of AI agent identities.

– Bare name with no further mechanism changelog-20261004-42bd0c0b

└──▷ **BREAKING ON UPGRADE**

! ThreatMetrix nodes have been renamed to LexisNexis Dynamic Decision Platform (DDP) nodes — any configuration or documentation referencing the old ThreatMetrix node names will need to be updated.

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

# DNSFilter

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> DNSFilter's Windows Roaming Client 3.8.15 adds split-horizon DNS fallback control, automatic ISP-interception bypass, and Active Directory dynamic DNS registration, alongside a new MSP branding page, cursor-based Query Log paging, and several smaller dashboard and UI fixes.

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

## 01 Local domain fallback control in Roaming Client NEW

90

Adds `LocalDomainFallbackEnabled` setting to the Windows Roaming Client to control whether unresolvable local-domain queries fall back to DNSFilter or stay on the network, enabling split-horizon and internal-zone isolation.

Prevent internal split-horizon or private-zone queries from ever leaking to DNSFilter when your local resolvers can't answer them.

```ini
LocalDomainFallbackEnabled = false
```

— Named config key with example value and clear purpose changelog-20261004-cf2dec36

## 02 VPN agent conflict handling in Classic DNS Filtering IMPROVED

65

Disable Roaming Clients for Conflicting VPN Agents in Classic DNS Filtering now applies to all devices, and VPN adapter traffic is left to the VPN.

— Names the setting and new scope of behavior changelog-20261004-cf2dec36

## 03 Roaming Client reads device info via Windows APIs IMPROVED

60

Roaming Client now reads device identity, OS version, and adapter DNS settings from Windows APIs instead of WMI, lowering WMI Provider Host CPU usage on all devices including ARM64 and accelerating startup.

— Clear before/after mechanism but nothing user actionable changelog-20261004-cf2dec36

THINNER COVERAGE BELOW

04 **ISP DNS interception fallback** NEW 55

Roaming Client now detects ISP DNS interception and automatically moves the query to the next protocol in the configured order (e.g., DNS-over-TLS) so sites load normally.

— Explains mechanism but no user-facing control named changelog-20261004-cf2dec36

05 **AD domain-joined dynamic DNS registration** NEW 55

Active Directory domain-joined devices in Transparent Proxy and PreCheck modes now register DNS records with the domain controller via secure dynamic updates.

— Named modes but behavior is automatic, no action needed changelog-20261004-cf2dec36

06 **Branding settings page for MSPs** NEW 55

Adds a Branding settings page for MSPs without a custom domain configured, replacing the legacy Whitelabel form, with automatic logo migration.

— Names replaced UI and migration behavior, gives a path changelog-20261004-cf2dec36

07 **Category display for non-category blocks** IMPROVED 50

Unblock Requests grid Category column now shows domain category information even when a domain was blocked for a non-category reason (Block List, AppAware, or Security block).

— Names the reasons affected but no action for reader changelog-20261004-cf2dec36

08 **Certificate warning removed on HTTPS block pages** IMPROVED 50

Blocked HTTPS sites now show the block page without a certificate warning on MSP organizations created after September 15.

— Specific date condition named but no config exposed changelog-20261004-cf2dec36

09 **Cursor-based Query Log pagination** IMPROVED 45

Query Log switches to cursor-based pagination, replacing page-number paging for stable forward/back navigation.

— States the mechanism change but no further detail changelog-20261004-cf2dec36

10 **License overage banners on Custom Dashboards** NEW 40

License overage warning and critical banners are now visible on Custom Dashboards.

— Brief statement with named surface, little mechanism changelog-20261004-cf2dec36

11 **Custom reason text in Diagnostic Tool** IMPROVED 30

Adds custom description input to the Diagnostic Tool when Other is selected as the reason.

— Thin, single-line UI addition changelog-20261004-cf2dec36

WAS THIS USEFUL? 👍 👎

## tailscale

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

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

> Tailscale's web-based access client now maintains a single authenticated session shared across all browser tabs, removing repeated sign-in prompts.

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

### 01 Single-session PAM web client at my.tailscale.com IMPROVED

65

Adds a single-session PAM web client at `my.tailscale.com` that runs as one shared browser-based Tailscale device across all tabs, so authenticating once covers every subsequent service connection in the same browser session.

Access multiple internal services in one browser session without re-authenticating for each tab.

> 📍 In your browser, navigate to `my.tailscale.com` and authenticate once. Then open additional tabs to other services on your tailnet — no further sign-in prompts will appear.

— Names exact URL and mechanism, lacks session duration or scope limits

changelog-20261004-48705c4b

WAS THIS USEFUL? 👍 👎

◆ Backup & Recovery

# Druva Data Resiliency Cloud

Feedback ⓘ

changelog · Sep 25, 2026 NOTES ↗ RANK

Druva Data Resiliency Cloud is a cloud-native platform providing backup, disaster recovery, and ransomware protection for enterprise data.

> Druva expanded its ServiceNow integration to new regions and introduced 30-day free trials for three additional workload types, accessible directly from the product console.

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

01 **Free trials for Okta, AD, Dynamics 365** NEW 65

Druva enables 30-day free trials for Okta, Active Directory, and Microsoft Dynamics 365 workloads, available to both new and existing customers via `login.druva.com/signup` or the product console's Workloads section.

Start a free trial of Okta, Active Directory, or Dynamics 365 data protection as an existing Druva customer without leaving your console.

> 📍 1. Log in to the Druva product console. 2. Navigate to the Workloads section. 3. Select Start Trial next to Okta, Active Directory, or Dynamics 365 (subject to regional availability).

— Names exact signup URL and console path, lacks trial mechanics detail

2026-09-25-fd009959

THINNER COVERAGE BELOW

02 **ServiceNow Australia Cloud and FedRAMP GovCloud support** NEW 30

The Druva ServiceNow integration now supports the Australia Cloud and FedRAMP GovCloud regions.

— Names regions but no setup steps or mechanism 2026-09-25-fd009959

WAS THIS USEFUL? 👍 👎

## Velero

Feedback ⓘ v1.18.3 NOTES ↗ RANK

Velero is an open-source tool that backs up, restores, and migrates Kubernetes cluster resources and persistent volumes.

> Velero v1.18.3 adds global backup volume policy enforcement, fine-grained resource-policy filters for both backup and restore, and support for encrypted CSI volumes in datamover backups, alongside smaller validation and error-reporting improvements.

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

### 01 Global backup volume policies and volume/access mode matching

NEW 85

Adds the `--global-backup-volume-policies-configmap` server flag to merge cluster-wide backup volume policies into every backup, and adds support for matching PVCs by volume mode and access mode in resource policies.

Apply a cluster-wide volume policy to every backup without repeating it per-backup — useful when enforcing encrypted-volume exclusion org-wide.

```
$ velero server --global-backup-volume-policies-
configmap=cluster-volume-policies
```

— Names exact flag and includes a runnable server command v1.18.3

### 02 Fine-grained filter policies for backup and restore NEW

80

Adds `ClusterScopedFilterPolicy` and `NamespacedFilterPolicy` sections to resource policy for fine-grained backup filters, and adds a `resourcePolicy` field to `restoreSpec` with the same `ClusterScopedFilterPolicy` and `NamespacedFilterPolicy` sections for fine-grained restore filters. A new `restore.velero.io/must-include-additional-items` annotation lets RestoreItemActions opt in to bypassing these global restore filters for AdditionalItems.

— Names all config fields and annotation but no runnable example v1.18.3

THINNER COVERAGE BELOW

### 03 Encrypted CSI volume support in datamover backups NEW

45

Supports copying namespace-scoped secrets and configmaps needed for backup and restore PVC provisioning, enabling datamover backup/restore of encrypted CSI volumes.

— Explains mechanism but no config surface or command named v1.18.3

04 **Backup validation requires running node-agent pods** IMPROVED

45

Fails backup validation when the built-in data mover is requested but no node-agent pods are running.

— Names exact failure condition but no flag or config key v1.18.3

05 **Operation context in error messages** IMPROVED

25

Adds operation context to user-facing error messages shown in CR statuses and CLI output.

— Vague improvement with no concrete example of new messages v1.18.3

WAS THIS USEFUL? 👍 👎

## Veeam Kasten

Feedback ⓘ 9.0.6 NOTES ↗ RANK

Veeam Kasten is a Kubernetes-native platform for backing up, restoring, and migrating containerized applications and their persistent data.

> Kasten K10 9.0.6 adds tunable Kubernetes API rate limits, expiry management for RestorePoints, and a technical-preview changed block tracking feature for VM backups, alongside Kubernetes 1.35 support and several breaking changes around deprecated Helm timeout keys and private registry credentials.

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

### 01 Configurable Kubernetes API client rate limits IMPROVED

90

Adds `kubeClient.qps` and `kubeClient.burst` Helm parameters to make Kubernetes API client rate limits configurable, with defaults raised from 20/50 to 50/100.

Tune Kasten's Kubernetes API client rate limits at install time to avoid throttling in large clusters.

```
$ helm upgrade k10 kasten/k10 --namespace kasten-io --set
kubeClient.qps=100 --set kubeClient.burst=200
```

— Named Helm flags, concrete default change, runnable upgrade command 9.0.6

### 02 Deprecated blueprint timeout Helm values DEPRECATED

80

The Helm values `timeout.blueprintBackup`, `timeout.blueprintRestore`, `timeout.blueprintDelete`, and `timeout.blueprintHooks` are deprecated and will be removed in a future release; replace them with `timeout.backup`, `timeout.restore`, `timeout.retire`, and `timeout.blueprintResourceHooks` respectively (old values still take priority if set).

— Exact old and new config keys with migration guidance 9.0.6

### 03 Private registry image pull failure on Kubernetes 1.35

80

BREAKING

On Kubernetes 1.35 or later, backup and restore of applications using a private container registry fails because worker pods have no image pull credentials in the application

namespace; a manual workaround is required — create the image pull secret in each protected namespace and attach it to the default service account.

— Root cause and exact manual workaround steps given 9.0.6

04 **Changed block tracking for VM backups** NEW 60

Adds changed block tracking for VM backups independent of underlying Kubernetes storage via the `VirtualMachineBackup` API, shipped as a Technical Preview.

— Names API and preview status but no usage detail 9.0.6

THINNER COVERAGE BELOW

05 **Kubernetes 1.35 support; 1.31 dropped** BREAKING 55

Adds support for Kubernetes 1.35, while support for Kubernetes 1.31 has been removed — clusters must be on Kubernetes 1.32 or later (OpenShift 4.18 continues to be supported).

— States exact version boundary but no migration steps 9.0.6

06 **Expiry management for RestorePoints** NEW 50

Adds support for setting, updating, and removing expiry on existing `RestorePoints` and `RestorePointContents` resources.

— Names resources but no command or workflow given 9.0.6

└──▷ **BREAKING ON UPGRADE**

! Support for Kubernetes 1.31 has been removed; clusters must be on Kubernetes 1.32 or later (OpenShift 4.18 continues to be supported).

! The Helm values `timeout.blueprintBackup`, `timeout.blueprintRestore`, `timeout.blueprintDelete`, and `timeout.blueprintHooks` are deprecated and will be removed in a future release; replace them with `timeout.backup`, `timeout.restore`, `timeout.retire`, and `timeout.blueprintResourceHooks` respectively (old values still take priority if set).

! On Kubernetes 1.35 or later, backup and restore of applications using a private container registry fails because worker pods have no image pull credentials in the application namespace — a manual workaround is required (create the image pull secret in each protected namespace and attach it to the default service account).

WAS THIS USEFUL? 👍 👎

## GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

## CISO Assistant

Feedback ⓘ v4.1.0 NOTES ↗

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

Adds MCP risk-review write tools, entity-assessment CSV/XLSX export, a `user-creator` builtin group, CEL `compute` workflow action, and an `asset-focus` whiteboard mode.

└──▷ GET THIS VERSION

```
$ git clone --branch v4.1.0 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v4.1.0
```

Adds `user-creator` builtin group to control which users can create new accounts.

Adds export of entity assessments to CSV and XLSX formats in the TPRM module.

Adds MCP risk-review write tools with actor resolution for automated risk-review workflows.

Adds `compute` action for CEL arithmetic expressions in workflows.

Adds `asset-focus` secondary mode to the asset whiteboard for an asset-centric view.

+2 more

NEW COMPLIANCE FRAMEWORK BSI C5 Criteria Catalogue 2026 framework (EN, DE)

WAS THIS USEFUL? 👍 👎

## PLATFORMS & UTILITIES

◆ General Utilities & Libraries

# Obsidian

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗ RANK

The free and flexible app for your private thoughts.

> Obsidian's latest release adds Quick Capture templates and new capture-location options, a Group control for Bases views, Quick Look previews for Markdown on macOS, and a full right-to-left workspace flip, alongside a round of theming, search, and accessibility improvements.

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

01 **Theming CSS variable prefixes** NEW 70

Adds `--tooltip-`, `--notice-`, `--hotkey`, `--tab-inner-`, and `--tab-container-` CSS variable prefixes for theming tooltips, notices, hotkeys, and tabs.

— All five variable prefixes named verbatim for direct theme use.

changelog-20261004-69756476

02 **Quick Capture templates and capture locations** NEW 65

Quick Capture on iOS now adds template support when its behavior is set to daily note or a selected note. Across platforms, Quick Capture adds Create Locations to capture to a new note, today's daily note, a bookmarked note, or any chosen note.

— Names every capture-location option; no exact settings path given.

changelog-20261004-69756476

03 **Open file from outside the vault** NEW 65

Adds the Open file from outside the vault... command, letting users pick and view any file on their computer in the app.

Open and view a file that lives outside your vault — useful for reviewing external config or log files without importing them.

> 📍 Open the Command Palette, search for Open file from outside the vault..., and select the target file on your computer.

— Exact command name plus runnable steps provided. changelog-20261004-69756476

04 **Group control for Bases toolbar** NEW 60

Adds a Group menu to the Bases toolbar for choosing the property to group by, with the ability to reorder, hide, and add groups manually in any view type.

— Names the menu and toolbar location, no command example. changelog-20261004-69756476

THINNER COVERAGE BELOW

05 **Right-to-left workspace flip** IMPROVED 55

The entire workspace, including sidebars, now flips when Obsidian is set to a right-to-left (RTL) language; the Toggle left sidebar command continues to refer to the visual left sidebar even when the interface is flipped.

— Explains before/after behavior but gives no setup steps. changelog-20261004-69756476

06 **Installer update notice in settings** NEW 50

Adds an update notice in Settings → General when a newer installer is available.

— Exact settings path named, straightforward to find. changelog-20261004-69756476

07 **Mobile photo capture from attachment toolbar** IMPROVED 45

The Insert attachment mobile toolbar button now allows taking a photo directly.

— Names exact toolbar button and new action. changelog-20261004-69756476

08 **Theme/snippet disabling for untrusted vaults** IMPROVED 45

When opening an untrusted vault, themes and snippets are temporarily disabled while the 'Do you trust the author of this vault' dialog is on screen.

— Describes the mechanism but no config toggle given. changelog-20261004-69756476

09 **Faster, smarter fuzzy search ranking** IMPROVED 45

Improves fuzzy search in the Quick switcher and suggestions: matches where typed letters start words now rank higher, and searching is faster in large vaults.

— Describes ranking and speed change without a demonstrable example. changelog-20261004-69756476

10 **Source mode ArrowUp moves to inline title** IMPROVED 45

In Source mode, pressing `ArrowUp` on the first line of a note now moves the cursor to the inline title, consistent with Live Preview behavior.

— Names the exact key and mode, a small consistency fix. changelog-20261004-69756476

11 **Quick Look previews for Markdown on macOS** NEW 40

Adds Quick Look previews for Markdown files on macOS (requires latest installer).

— States the requirement but no usage steps. changelog-20261004-69756476

12 **Font size commands** NEW 40

Adds Increase font size and Decrease font size commands.

— Named commands usable directly via the Command Palette. changelog-20261004-69756476

13 **Document icons for vault file types** NEW 35

Adds document icons on macOS and Windows for `.md`, `.base`, and `.canvas` files.

— Lists affected file types only, no further detail. changelog-20261004-69756476

14 **New base/canvas shortcuts in empty state** NEW 35

Adds New base and New canvas shortcuts to the redesigned empty state when their respective plugins are enabled.

— Thin description of UI shortcuts and their plugin dependency.

changelog-20261004-69756476

15 **System text size scaling** IMPROVED 30

Text and interface elements now scale with the system's preferred text size, including larger accessibility sizes.

— General accessibility claim without specifics. changelog-20261004-69756476

16 **Local-only storage, no Obsidian Sync** BREAKING 30

Obsidian is now stored in the device's local storage and no longer syncs with Obsidian Sync.

— States the change but is vague on what exactly stopped syncing.

changelog-20261004-69756476

## └──▷ ALSO FROM THESE RELEASES

Exclude an entire folder and its contents from File Explorer search results by prefixing the folder name with a minus sign.

📍 In the File Explorer search box, type: `-Archive`

WAS THIS USEFUL? 👍 👎

## INFRASTRUCTURE

◆ Internet Services

# Cloudflare

Feedback ⓘ changelog · Oct 4, 2026 CHANGELOG ↗

RANK

Connect, protect, and build everywhere.

> Cloudflare shipped a beta Web Search API for AI Gateway-backed agents, a durable Pi agent harness, deterministic request sampling in Rules, GA jurisdiction-locked KV namespaces, and tightened Zero Trust service-token authentication that is now mandatory for new organizations.

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

## 01 Strict service token authentication in Access

BREAKING

88

Adds a `strict_service_token_auth` field to the `PATCH https://api.cloudflare.com/client/v4/accounts/{account_id}/access/organizations` endpoint to enforce consistent service-token-only authentication in Cloudflare Access. Zero Trust organizations created on or after October 5, 2026 have this enabled by default and cannot disable it: requests carrying service token headers are never redirected to the login page, Allow policies are ignored, and no `CF_Authorization` cookie is issued on authenticated requests.

Enable strict service token authentication for an existing Zero Trust organization so that service-token requests are never redirected to login and Allow policies are bypassed.

```
$ curl -X PATCH
'https://api.cloudflare.com/client/v4/accounts/{account_id}/acces
s/organizations' \
  -H 'Authorization: Bearer $CLOUDFLARE_API_TOKEN' \
  -H 'Content-Type: application/json' \
  --json '{"strict_service_token_auth": true}'
```

— Endpoint, field, default behavior and exact PATCH call given

changelog-20261004-05f0da5b

## 02 Web Search API (beta) via AI Gateway

NEW

84

Introduces the Web Search API (beta) at `/{account_id}/ai/websearch/`, supporting `query`, `provider` (`ceramic`, `exa`, `linkup`), `limit`, and `options.gateway.id` parameters, routing search requests through AI Gateway with Zero Data Retention.

Query the Web Search API from the CLI to ground an AI agent's response in live web results via AI Gateway.

```
$ curl
https://api.cloudflare.com/client/v4/accounts/$CLOUDFLARE_ACCOUNT
_ID/ai/websearch/ \
  -H 'Authorization: Bearer $CLOUDFLARE_API_TOKEN' \
  -H 'Content-Type: application/json' \
  --data '{"query": "latest CVEs in OpenSSL", "provider": "exa",
"limit": 5, "options": {"gateway": {"id": "default"}}}'
```

— Full endpoint, params, and runnable curl example given `changelog-20261004-05f0da5b`

03 **KV namespace data-residency jurisdictions** IMPROVED

70

Workers KV namespaces can be created with a jurisdiction lock, e.g. `wrangler@latest kv namespace create NAMESPACE_NAME --jurisdiction=eu`, to satisfy EU data-localization requirements; this reaches general availability in this window.

Create a Workers KV namespace locked to EU data residency to satisfy GDPR data-localization requirements.

```
$ wrangler@latest kv namespace create NAMESPACE_NAME --
jurisdiction=eu
```

— Runnable CLI flag given but GA status only in summary `changelog-20261004-05f0da5b`

THINNER COVERAGE BELOW

04 **PiHarness durable agent class in Agents SDK** NEW

59

Adds a `PiHarness` class to the Cloudflare Agents SDK (`agents/harness/pi`) for building durable long-running AI agents using the Pi 1.0 / Pi Durable harness, with support for tools, extensions, and lifecycle persistence in Durable Objects.

— Names class and module but gives no usage example `changelog-20261004-05f0da5b`

05 **hash_in_range() for percentage-based rule sampling** NEW

56

Adds the hash_in_range() function to Cloudflare Rules expressions across all plans and HTTP products, enabling deterministic percentage-based request sampling using `cf.random_seed`.

— Function and parameter named, no example of use `changelog-20261004-05f0da5b`

06 **30-day analytics retention for all plans** IMPROVED 23

Cloudflare now provides 30-day analytics retention for all plans.

— Only mentioned in passing, no mechanism or scope changelog-20261004-05f0da5b

└──▷ **ALSO FROM THESE RELEASES**

.
.
.

└──▷ **BREAKING ON UPGRADE**

! Zero Trust organizations created on or after October 5, 2026 have `strict_service_token_auth` enabled by default and cannot disable it — requests with service token headers will never be redirected to the login page, Allow policies are ignored, and no `CF_Authorization` cookie is returned.

---

WAS THIS USEFUL? 👍 👎

## OTHER / UNCATEGORIZED

◆ UNCATEGORIZED

# vigolium

Feedback ⓘ v0.5.2 NOTES ↗ RANK

Vigolium - High-fidelity vulnerability scanner fusing agentic AI with native speed, modularity, and precision

> Vigolium v0.5.2 adds new scan completeness and event diagnostics fields, several opt-in CLI flags for auth-gating, database recovery and glob/output control, and ships multiple breaking changes to the browser crawler's default behaviour, JSON output structure, and crawl graph file naming.

└──▷ **WHAT SHIPPED · 15 FEATURES** most completely described first ? what's the number?

01 **Auth-gating with --require-auth** NEW 85

Adds `--require-auth` flag and `spidering.require_auth` config key so a failed login is fatal for that target, preventing anonymous crawl data from being collected for authenticated targets.

Fail a scan immediately when the login step is unsuccessful, ensuring no anonymous crawl data is collected for authenticated targets.

```
$ vigolium scan-url https://app.example.com --require-auth
```

— Flag, config key, mechanism and runnable command all given v0.5.2

02 **JSON output format restructured to items array** BREAKING 83

`-j` now emits one document per invocation with `items` as the only row array, replacing the previous per-command row array names; the new `--json-legacy-keys` flag restores the old per-command row arrays for scripts that depend on them.

— Names old and new format plus the migration flag v0.5.2

03 **Database recovery on failed scans** NEW 80

Adds `--keep-db-on-error` flag to preserve a failed `-S` run's database under `~/.vigolium/recovered/` instead of deleting it.

Recover the database from a failed session-based scan for post-mortem triage instead of having it deleted.

```
$ vigolium scan-url https://app.example.com -S session.db --keep-db-on-error
```

— Flag, path and runnable command all given v0.5.2

04 **Crawl graph filename format changed** BREAKING 78

Crawl graph filenames are now `crawl-graph-<host>-<scan>-<seq>.json` (redacted and owner-only); any glob targeting the old filename pattern must be updated.

— Exact new filename pattern and migration note given v0.5.2

05 **Browser crawler interaction restrictions** BREAKING 75

The browser crawler no longer creates accounts, uploads, or downloads files, and now cancels confirm() dialogs by default; the new `spidering.interaction.*` config keys restore each of these behaviours individually.

— Clear before/after behaviour and the restoring config key v0.5.2

06 **NDJSON event stream now exclusive and sequenced** IMPROVED 70

Makes `--events ndjson` own stdout exclusively, with events carrying a `seq` field and a terminal event written after finalization.

— Flag and new event fields named with behaviour explained v0.5.2

07 **Scan completeness and event diagnostics fields** NEW 68

Adds `completeness`, `stop_reason`, and `phase_outcomes` fields to the scan row, REST object, and `--format jsonl` output, plus `reasons` and `limits` fields on `phase.finished` and `scan.finished` events, with `stop_reason` also added to the scan line.

— Names exact fields and surfaces but no worked example v0.5.2

08 **Strict glob-db accounting** NEW 65

Adds `--glob-strict` flag for `--glob-db` reads, with `glob_sources` accounting naming every skipped file.

— Flag named, no usage example provided v0.5.2

09 **Export failures now hard-fail** BREAKING 65

Exits 1 with `error.code: "export_failed"` when a requested output cannot be written, instead of warning.

— Exact error code and new exit behaviour given v0.5.2

10 **Output byte limits on CLI commands** NEW 60

Adds `--max-output-bytes` (opt-in) flag on `finding`, `traffic`, and `db ls` commands.

— Flag and target commands named but behaviour thin v0.5.2

11 **Browser sandbox enabled by default** BREAKING 60

Enables the browser sandbox by default; the `--browser-insecure` flag restores the previous posture.

— Default change and revert flag named, little mechanism v0.5.2

THINNER COVERAGE BELOW

12 **Atomic single-file output publishing** IMPROVED 55

Makes single-file `-o` outputs publish atomically, leaving the previous file intact on failure.

— Mechanism stated but no flag or example given v0.5.2

13 **Browser conformance test target** NEW 50

Adds `make test-browser-conformance` target running a browser conformance suite with a launch precheck.

— Command named but suite contents unspecified v0.5.2

14 **New spidering identity and capture config keys** NEW 45

Adds `spidering.identity_email_domain`, `spidering.graph_include_values`, and `spidering.max_capture_body_bytes` config keys.

— Keys named but purpose and effect unexplained v0.5.2

15 **SIGTERM cancels running scans** IMPROVED 35

Enables SIGTERM to cancel a scan the same way Ctrl-C does.

— Behaviour stated with no further mechanism or example v0.5.2

└──▷ **BREAKING ON UPGRADE**

! The browser crawler no longer creates accounts, uploads or downloads files, and now cancels confirm() dialogs by default; `spidering.interaction.*` restores each behaviour individually.

! Crawl graph filenames are now `crawl-graph-<host>-<scan>-<seq>.json` (redacted and owner-only); any glob targeting the old filename pattern must be updated.

! `-j` now emits one document per invocation with `items` as the only row array; scripts relying on the old per-command row array names must pass `--json-legacy-keys` or be updated.

---

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 4, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue