THE CYBER TOOLCHAIN

NO. 091

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 1, 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 117 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 20 tools

▾ // THE BRIEF HIDE

What stands out across today's releases, grouped by what it lets you do. Every tool named links to its entry below.

Three unrelated things stand out. 1Password's NVIDIA OpenShell beta hands sandboxed agents placeholders instead of real secrets, so a promised agent leaks nothing usable. code-oss now runs agent

vim ? help

terminal sessions inside an OS-level sandbox rather than trusting them with your shell. And JumpCloud's Shadow AI Dashboard puts unsanctioned AI tool usage next to the rest of the SaaS inventory.

PROTECT

Let an AI agent use a credential without ever handing it the credential

1Password injects placeholders into sandboxed agent calls so the real secret never enters the agent's context window or logs, and code-oss confines Local and Copilot Agent Host terminal sessions at the OS level instead of giving them the user's full shell. Operant AI's label-aware plugin blocking reads Purview sensitivity labels, so a Copilot plugin can be denied data it was never cleared for rather than relying on after-the-fact detection.

1Password · code-oss · Operant AI

IDENTIFY

See which AI tools your staff are actually using before the policy conversation

JumpCloud's Shadow AI Dashboard sits inside the new SaaS Management suite, so unsanctioned AI usage shows up in the same inventory as the rest of the app sprawl rather than in a separate point tool. Nudge Security's AI Risk Agents go further and remediate risky OAuth grants and browser extensions, the two paths by which a staff-installed tool quietly acquires mailbox or drive scope.

JumpCloud · Nudge Security

PROTECT

Grant access to a system you don't own the IdP for, and let the customer configure it

Clerk moves Directory Sync setup, Google Workspace included, into the Organization Profile component, so an enterprise customer's IT admin wires up their own provisioning without filing a ticket with your engineers. P0 Security's new Salesforce, Cloudflare, Grafana Cloud and Datadog connectors bring those consoles under runtime access control, which is where standing admin seats normally accumulate unnoticed; Keycloak promotes its SCIM API toward GA for the de-provisioning side.

Clerk

◆ SAST / SCA / Code Security

GitHub

Feedback ⓘ

Opt-in dist-tag permissions for npm trusted publishing (2026-09-30) BLOG ↗

RANK

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

> GitHub shipped OIDC-based dist-tag management for npm trusted publishing, opened self-serve GitHub Advanced Security trials to GitHub Team orgs, and expanded the HydraFusion multi-model orchestrator into VS Code and the Copilot app.

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

01 HydraFusion expands to VS Code and Copilot app IMPROVED

82

HydraFusion, previously limited to Copilot CLI, is now available in VS Code (version 1.140+, including Insiders) and the GitHub Copilot app. It adds three selectable orchestration workflows — Single, Cascade, and Critique — where HydraFusion picks the most efficient execution pattern per task rather than routing to one model, plus real-time, more frequent progress updates during long-running tasks. If it doesn't appear automatically in VS Code's Copilot Chat model picker, it can be activated via `chat.copilot.hydraFusion.enabled` in settings.

Enable HydraFusion in VS Code when it does not appear in the model picker — useful for early adopters or orgs where the feature is not yet visible by default.

```json
chat.copilot.hydraFusion.enabled
```

Turn on HydraFusion in the GitHub Copilot app to access multi-model orchestration on mobile or desktop outside VS Code.

> 📍 In the GitHub Copilot app: go to Settings, search for HydraFusion, turn it on, then select HydraFusion from the model picker.

— Names config key, version requirement, workflow modes, and enable steps.

HydraFusion in VS Code and the GitHub C…

02 Dist-tag permissions for npm trusted publishing NEW

81

Adds an opt-in `Allow npm dist-tag` permission to each trusted publishing configuration, letting CI promote to `latest` or update `next` / `beta` pointers via short-lived OIDC credentials instead of a long-lived npm token. Staging-only configurations can independently receive this permission without needing direct publish access, and a dist-tag operation is authorized if the incoming OIDC token matches any configuration with `Allow npm dist-tag` enabled; existing token-based dist-tag management is unchanged.

Enable OIDC-based dist-tag management on a package so CI can promote a release to `latest` without storing a long-lived npm token.

> 📍 In your package's trusted publishing settings, locate the configuration that handles releases, then enable `Allow npm dist-tag` on that configuration.

— Names exact permission and mechanism; UI steps given but no CLI/API path.

`Opt-in dist-tag permissions for npm tru…`

---

03 **Self-serve GitHub Advanced Security trials for GitHub Team**

NEW 66

GitHub Team customers can now start a self-serve trial of GitHub Advanced Security — covering GitHub Code Security and GitHub Secret Protection — without contacting sales, from the organization Overview page, the Billing and licensing > Licensing page, or the Risk Assessment completion page.

Start a GitHub Advanced Security trial directly from your organization's billing settings without contacting sales.

> 📍 In your GitHub organization, go to Settings › Billing and licensing › Licensing, then select `Start trial` under GitHub Advanced Security.

— Names exact products and three entry points; clear navigation given.

`GitHub Advanced Security trials for Git…`

`Opt-in dist-tag permissions for npm trusted publishing (2026-09-30)` BLOG ↗

LATEST STABLE

GitHub npm trusted publishing now supports opt-in dist-tag management via short-lived OIDC credentials, eliminating the last long-lived token requirement.

└──▷ **HOW TO FIND IT**

Enable OIDC-based dist-tag management on a package so CI can promote a release to `latest` without storing a long-lived npm token.

> 📍 In your package's trusted publishing settings, locate the configuration that handles releases, then enable `Allow npm dist-tag` on that configuration.

Adds an opt-in `Allow npm dist-tag` permission to each trusted publishing configuration, enabling dist-tag operations (promoting to `latest`, updating `next` and `beta` pointers) via short-lived OIDC credentials instead of a long-lived access token.

Allows staging-only trusted publishing configurations to independently receive dist-tag management permission, without requiring direct publish access.

Authorizes a dist-tag operation when the incoming OIDC token matches any one configuration that has `Allow npm dist-tag` enabled, leaving existing token-based dist-tag management unchanged.

`GitHub Advanced Security trials for GitHub Team (2026-09-30)` `BLOG ↗` `STABLE`

GitHub Team orgs can now self-serve trial GitHub Advanced Security (Code Security + Secret Protection) without contacting sales.

└──▷ **HOW TO FIND IT**

Start a GitHub Advanced Security trial directly from your organization's billing settings without contacting sales.

📍 In your GitHub organization, go to Settings › Billing and licensing › Licensing, then select `Start trial` under GitHub Advanced Security.

`HydraFusion in VS Code and the GitHub Copilot app (2026-09-30)` `BLOG ↗` `STABLE`

HydraFusion multi-model orchestrator expands to VS Code and the GitHub Copilot app, adding cascade and critique workflows.

└──▷ **USE IT**

Enable HydraFusion in VS Code when it does not appear in the model picker — useful for early adopters or orgs where the feature is not yet visible by default.

.vscode/settings.json

```
chat.copilot.hydraFusion.enabled
```

Turn on HydraFusion in the GitHub Copilot app to access multi-model orchestration on mobile or desktop outside VS Code.

📍 In the GitHub Copilot app: go to Settings, search for `HydraFusion`, turn it on, then select HydraFusion from the model picker.

Enables `chat.copilot.hydraFusion.enabled` in VS Code 1.140+ to activate HydraFusion from the Copilot Chat model picker when it does not appear

automatically.

Adds HydraFusion to VS Code (version 1.140 or later, including VS Code Insiders) and the GitHub Copilot app, expanding beyond Copilot CLI.

Introduces three selectable orchestration workflows — Single, Cascade, and Critique — where HydraFusion picks the most efficient execution pattern per task instead of routing to a single model.

Adds real-time, more frequent progress updates so practitioners can track HydraFusion workflow steps and status during long-running tasks.

WAS THIS USEFUL?  

NETWORK SECURITY

◆ Firewalls & Network Defense

Fastly

Feedback ⓘ

Automation tokens now support multiple roles (2026-09-24) BLOG ↗ RANK

Fastly's edge cloud platform delivers faster, safer, and more scalable sites and apps to customers. Elevate your edge CDN, video delivery, security, and more.

> Fastly automation tokens can now carry multiple roles at once, letting a single token combine permissions across products like CDN management and Next-Gen WAF.

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

01 **Multi-role automation tokens** IMPROVED 45

Automation tokens now support assigning multiple roles to a single token via the Automation Tokens API, enabling combined permissions across Fastly products such as CDN management and Next-Gen WAF.

— Names the API and use case but no endpoint or field details

Automation tokens now support multiple …

> Automation tokens now support multiple roles (2026-09-24) BLOG ↗ LATEST
>
> STABLE
>
> Fastly automation tokens now support multiple roles for fine-grained access control across CDN and Next-Gen WAF.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SIEM

Cisco Splunk Enterprise

Feedback ⓘ

changelog · Oct 1, 2026 NOTES ↗ RANK

Splunk Enterprise enables you to search, analyze and visualize your data to quickly act on insights from across your technology landscape.

> Splunk Enterprise 10.6 ships FIPS-compliant secret re-encryption, replaces the KV store backend with PostgreSQL, adds mTLS for Federated Search, expands Edge Processor pipeline capabilities with new SPL2 commands and a raw HEC endpoint, and introduces configuration audit logging, SCIM user de-provisioning and ARM64 support — alongside breaking changes to TLS and Federated Search version requirements.

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

01 **FIPS-compliant secret re-encryption** NEW 88

Adds `splunk reencrypt secrets` and `splunk reencrypt shcluster-secrets` CLI commands to migrate encrypted configuration values from the `$7$` cipher format to the new FIPS-compliant `$8$` cipher format using HKDF-SHA256.

Migrate all non-8 encrypted secrets on a standalone Splunk Enterprise instance to the new FIPS-compliant 8 cipher format after upgrading to 10.6.

```
$ splunk reencrypt secrets
```

Migrate encrypted secrets across all members of a search head cluster to the 8 cipher format in one step.

```
$ splunk reencrypt shcluster-secrets
```

— Names exact CLI commands and cipher/algorithm, fully runnable 2026-10-01-9287d00c

02 **No-restart app uninstall via reload_on_delete** NEW 81

Adds `[reload_on_delete]` stanza with `disabled = false` / `disabled = true` toggle in `limits.conf` to enable no-restart app uninstall operations, reducing restart requirements by roughly 50%.

Enable no-restart app uninstall on Splunk Enterprise 10.6 to reduce operational disruption when removing apps.

```ini
[reload_on_delete]
disabled = false
```

— Config key, file path and before/after metric given 2026-10-01-9287d00c

03 **Edge Processor SPL2 pipeline enhancements** NEW 80

Edge Processor pipelines gain stateful aggregation via the `stats` SPL2 command within a configurable state window, deduplication via the `dedup` command, conditional handling via the `if` command, and conversion functions `array_to_csv`, `csv_to_array`, `kv_keys`, `kv_to_object`, `object_to_csv`, and `object_to_kv`; pipelines can also send raw data to Splunk indexes via the `services/collector/raw` HTTP Event Collector endpoint.

— Names every SPL2 command, function and endpoint added 2026-10-01-9287d00c

04 **TLS 1.0 and 1.1 removal for inter-component connections** 60

BREAKING

TLS 1.0 and TLS 1.1 are no longer supported for inter-Splunk component connections and cannot be re-enabled; deployments must use TLS 1.2 or 1.3.

— States exact before/after versions and that it's irreversible 2026-10-01-9287d00c

THINNER COVERAGE BELOW

05 **PostgreSQL-backed KV store** IMPROVED 55

Replaces the MongoDB-backed KV store with a PostgreSQL-backed co-hosted KV store on supported Linux, Windows, and macOS platforms, preserving existing KV store APIs and application workflows.

— Explains backend swap and compatibility but no setup steps 2026-10-01-9287d00c

06 **Configuration change audit logging** NEW 50

Adds configuration change tracking via audit logs in the `_audit` index for Splunk Enterprise, recording who changed what and when via Splunk Web or the REST API.

— Names the index and access paths but no query example 2026-10-01-9287d00c

07 **ARM64 (aarch64) platform support** NEW 50

Adds support for running Splunk Enterprise on `aarch64` (ARM64) processor architecture, including AWS Graviton 4 VMs, in FIPS 140-3 mode, with conditional availability.

— Names architecture and FIPS mode but no deployment detail 2026-10-01-9287d00c

08 **Federated Search minimum version requirement** BREAKING

50

Federated searches will fail if any remote search head runs a version lower than Splunk Enterprise 10.4 after upgrading; all remote search heads must be upgraded to Splunk Enterprise 10.4 or higher before upgrading the deployment.

— Gives exact version threshold and upgrade order needed 2026-10-01-9287d00c

09 **SCIM auto-deprovisioning for Entra ID SAML users** NEW

45

Adds SCIM-based automatic user de-provisioning for Microsoft Entra ID SAML users, removing users from Splunk search heads when deleted from Entra ID or when Splunk access is revoked.

— Clear trigger conditions but no setup instructions 2026-10-01-9287d00c

10 **mTLS for Federated Search Hybrid Model** NEW

43

Adds mTLS (mutually-authenticated TLS) protocol support for Federated Search - Hybrid Model, requiring a client certificate installed on the Splunk Cloud Platform deployment.

— Names the feature and requirement but no config steps 2026-10-01-9287d00c

11 **Edge Processor management UI additions** NEW

40

Adds the ability to delete disconnected Edge Processor instances from the Edge Processor details page, and to choose the default telemetry indexer during Edge Processor first-time setup.

— UI paths given but behavior described only briefly 2026-10-01-9287d00c

└──▷ **BREAKING ON UPGRADE**

! Federated searches will fail if any remote search head runs a version lower than Splunk Enterprise 10.4 after upgrading; all remote search heads must be upgraded to Splunk Enterprise 10.4 or higher before upgrading the deployment.

! TLS 1.0 and TLS 1.1 are no longer supported for inter-Splunk component connections and cannot be re-enabled; deployments must use TLS 1.2 or 1.3.

changelog · Oct 1, 2026 NOTES ↗ LATEST STABLE

Splunk Enterprise 10.6 adds 8 FIPS-compliant encryption, PostgreSQL-backed KV store, mTLS Federated Search, and Edge Processor aggregation/dedup

└──▷ **TRY IT**

Migrate all non-8 encrypted secrets on a standalone Splunk Enterprise instance to the new FIPS-compliant 8 cipher format after upgrading to 10.6.

```
$ splunk reencrypt secrets
```

Migrate encrypted secrets across all members of a search head cluster to the 8 cipher format in one step.

```
$ splunk reencrypt shcluster-secrets
```

Enable no-restart app uninstall on Splunk Enterprise 10.6 to reduce operational disruption when removing apps.

```
$SPLUNK_HOME/etc/system/local/limits.conf
[reload_on_delete]
disabled = false
```

Adds `splunk reencrypt secrets` and `splunk reencrypt shcluster-secrets` CLI commands to migrate encrypted configuration values from the `$7$` cipher format to the new FIPS-compliant `$8$` cipher format (HKDF-SHA256).

Adds `[reload_on_delete]` stanza with `disabled = false` / `disabled = true` toggle in `limits.conf` to enable no-restart app uninstall operations, reducing restart requirements by ~50%.

Replaces MongoDB-backed KV store with a PostgreSQL-backed co-hosted KV store on supported Linux, Windows, and macOS platforms, preserving existing KV store APIs and application workflows.

Adds mTLS (mutually-authenticated TLS) protocol support for Federated Search - Hybrid Model, requiring a client certificate installed on the Splunk Cloud Platform deployment.

Adds stateful aggregation of Edge Processor pipeline events via the `stats` SPL2 command within a configurable state window.

+9 more

└──▷ **BREAKING ON UPGRADE**

! Federated searches will fail if any remote search head runs a version lower than Splunk Enterprise 10.4 after upgrading; all remote search heads must be upgraded to Splunk Enterprise 10.4 or higher before upgrading the deployment.

! TLS 1.0 and TLS 1.1 are no longer supported for inter-Splunk component connections and cannot be re-enabled; deployments must use TLS 1.2 or 1.3.

WAS THIS USEFUL?  

Databricks

Feedback ⓘ

Query tags for SQL warehouses are now generally available (2026-09-30) BLOG ↗

RANK

Databricks is a unified analytics platform for data engineering, data science, and machine learning built on Apache Spark.

> Databricks shipped GA for query tags on SQL warehouses and for Lakeflow Jobs table update triggers on OpenSharing objects and system tables, alongside a Postgres extension update for Lakebase and a new Simba JDBC driver release with Java 25 support.

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

01 **Query tags for SQL warehouses** NEW 70

Adds custom key-value query tags to SQL workloads on Databricks SQL warehouses and Lakehouse//RT compute, surfaced in `system.query.history` and the Query History page, enabling grouping, filtering, and cost attribution.

– Names the table and UI page but no tagging syntax shown.

Query tags for SQL warehouses are now g…

THINNER COVERAGE BELOW

02 **Lakeflow Jobs triggers on OpenSharing and system tables** NEW 50

Lakeflow Jobs table update triggers are now generally available for OpenSharing objects and system tables, enabling event-driven pipelines on shared and platform-managed data sources.

– Names trigger scope but omits setup or configuration steps.

Table update triggers on OpenSharing ob…

03 **Simba JDBC Driver 2.8.4 adds Java 25 support** IMPROVED 35

The Databricks JDBC Driver (Simba, Legacy) `2.8.4` now supports Java 25.

– Names exact driver version and Java target, no other detail.

Databricks JDBC Driver (Simba) 2.8.4 is…

04 **Updated Postgres extension versions in Lakebase** IMPROVED 10

Supported Postgres extensions for Lakebase have been updated to new versions.

— No extension names, old/new versions, or scope given.

Supported Postgres extensions updated t…

└──▷ ALSO FROM THESE RELEASES

Query tags for SQL warehouses are now generally available (2026-09-30) BLOG ↗

STABLE

Query tags for SQL warehouses are now GA, enabling custom key-value cost attribution visible in `system.query.history` and the UI.

Table update triggers on OpenSharing objects and system tables are now generally avail

BLOG ↗ LATEST STABLE

Lakeflow Jobs table update triggers now GA for OpenSharing objects and system tables on Databricks.

Databricks JDBC Driver (Simba) 2.8.4 is available (2026-09-29) BLOG ↗

STABLE

Databricks JDBC Driver (Simba) 2.8.4 adds Java 25 support.

WAS THIS USEFUL? 👍 👎

Sumo Logic

Feedback ⓘ

Apps, Solutions, and Collection Integrations - September Release (2026-09-30)

BLOG ↗ RANK

Sumo Logic is a cloud-based platform for log management, monitoring, and security analytics of applications and infrastructure.

> Sumo Logic rewrote its AWS Observability app as a Terraform-deployable v3.0.0 with expanded region coverage and next-generation dashboards, while expanding Automation Service actions across Azure AD, Cloud SIEM, CrowdStrike, AWS CloudWatchLogs and four new integrations, and migrating Microsoft Graph Security alert actions to a new, non-equivalent API ahead of a legacy endpoint's retirement.

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

01 AWS Observability app rewritten as v3.0.0 IMPROVED

85

AWS Observability v3.0.0 is a full rewrite adding Terraform Module support for AWSO solution deployment including release versioning, expanded AWS region support to non-SAM regions plus three newly supported regions (Asia Pacific Melbourne, Asia Pacific New Zealand, Europe Zurich), automatic configuration of appropriate Load Balancer policies for AWS regions launched after August 2022, and next-generation application support with out-of-the-box dashboards, monitors, FERs, and metric rules.

— Names Terraform module, specific regions and dashboard types, no exact commands.

AWS Observability Version 3.0.0 (Apps) …

02 Microsoft Graph Security migrates to alerts_v2 API BREAKING

85

Migrates the Get Alert, Search Alerts, and Update Alert actions in the Microsoft Graph Security integration to the new `alerts_v2` API. The legacy `/security/alerts` endpoint is deprecated and will be retired on October 15, 2026; `alerts_v2` is not a one-to-one replacement, so some alerts may be unavailable through the new endpoint.

— Gives endpoint, retirement date, and caveat but no migration steps.

Apps, Solutions, and Collection Integra…

03 Delegated auth and actions for Azure AD integration NEW

80

Adds Delegated (Device Code Flow) authentication support to the Azure AD integration alongside existing Application (Client Credentials) auth, along with new Initiate

Delegated Auth , Exchange Device Code , and Reset User Password With Writeback actions, plus new resource fields Authentication Type and Delegated Refresh Token .

– Names actions and fields but no exact UI path or endpoint.

Apps, Solutions, and Collection Integra…

04 **CrowdStrike Falcon Sandbox integration gains action and OAuth2 auth**

NEW

60

Adds a Check Submission Status action and OAuth 2.0 (Client Credentials) authentication support to the CrowdStrike Falcon Sandbox integration.

– Names action and auth type, no further mechanism detail.

Apps, Solutions, and Collection Integra…

THINNER COVERAGE BELOW

05 **Metric actions added to AWS CloudWatchLogs integration** NEW

55

Adds Get Metric Data , List Metrics , and Get Metric Statistics metric actions to the AWS CloudWatchLogs integration.

– Names three actions but no parameters or usage detail.

Apps, Solutions, and Collection Integra…

06 **New actions for Cloud SIEM Automation Service integration**

NEW

50

Adds Get Insight Triage and Check Insight Triage Schedule actions to the Sumo Logic Cloud SIEM Automation Service integration.

– Names two actions without further behaviour described.

Apps, Solutions, and Collection Integra…

07 **Filtering support for 1Password List Users action** IMPROVED

45

Adds filtering support to the List Users action in the 1Password integration.

– Names the exact action but not the filter parameters.

Apps, Solutions, and Collection Integra…

08 **Four new Automation Service integrations** NEW

40

Adds four new Automation Service integrations: AWS DynamoDB, Intel 471, Verity, and Mimecast V2.

– Names integrations only; no actions or setup detail given.

Apps, Solutions, and Collection Integra…

└──▷ **BREAKING ON UPGRADE**

! The Microsoft Graph Security legacy `/security/alerts` endpoint is deprecated and will be retired on October 15, 2026; `Get Alert`, `Search Alerts`, and `Update Alert` now call `alerts_v2`, which is not a one-to-one replacement — some alerts may be unavailable through the new endpoint.

`Apps, Solutions, and Collection Integrations - September Release (2026-09-30)`

`BLOG ↗` **LATEST** `STABLE`

Sumo Logic adds four new Automation Service integrations and expands Azure AD, CrowdStrike, and Cloud SIEM actions.

Adds `Initiate Delegated Auth`, `Exchange Device Code`, and `Reset User Password With Writeback` actions to the Azure AD integration under Delegated (Device Code Flow) auth, plus new resource fields `Authentication Type` and `Delegated Refresh Token`.

Adds Delegated (Device Code Flow) authentication support to the Azure AD integration alongside existing Application (Client Credentials) auth.

Adds `Get Insight Triage` and `Check Insight Triage Schedule` actions to the Sumo Logic Cloud SIEM Automation Service integration.

Adds `Check Submission Status` action and OAuth 2.0 (Client Credentials) authentication support to the CrowdStrike Falcon Sandbox integration.

Adds `Get Metric Data`, `List Metrics`, and `Get Metric Statistics` metric actions to the AWS CloudWatchLogs integration.

`+3 more`

└──▷ **BREAKING ON UPGRADE**

! The Microsoft Graph Security legacy `/security/alerts` endpoint is deprecated and will be retired on October 15, 2026; `Get Alert`, `Search Alerts`, and `Update Alert` now call `alerts_v2`, which is not a one-to-one replacement — some alerts may be unavailable through the new endpoint.

`AWS Observability Version 3.0.0 (Apps) (2026-09-22)` `BLOG ↗` `STABLE`

AWS Observability v3.0.0 delivers a full rewrite with expanded region coverage, Terraform Module deployment, and next-gen app dashboards.

Adds Terraform Module support for AWSO solution deployment, including release versioning.

Expands AWS region support to non-SAM regions and three newly supported regions: Asia Pacific (Melbourne), Asia Pacific (New Zealand), and Europe (Zurich).

Automatically configures appropriate Load Balancer policies for AWS regions launched after August 2022.

> Adds next-generation application support with out-of-the-box dashboards, monitors, FERs, and metric rules.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Trend Vision One

Feedback ⓘ

File Security Storage has released template version 2.3.1 for Google Cloud (2026-10-01)

BLOG ↗ RANK

Trend Vision One is Trend Micro's cloud-based XDR platform providing unified security visibility and threat detection across endpoints, networks, and cloud environments.

> Trend Vision One expanded File Security Storage's Scan Activity visibility across GCP, Azure, and AWS templates, added a configurable archive inspection limit, and brought Workbench alert triage and Case Management into the TrendAI Vision One Mobile app.

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

01 **extractFileCountLimit for archive scanning** NEW 76

The AWS File Security Storage template v4.5 adds an `extractFileCountLimit` parameter to control the maximum number of files inspected within a compressed archive, with a default of 30.

Raise the per-archive file inspection limit when your workload regularly processes large compressed archives with more than 30 files.

```yaml
extractFileCountLimit: 100
```

— Exact config key, default value, and usage example given

File Security Storage has released temp…

02 **Scan Activity filtering and detail in File Security Storage**

IMPROVED 69

The Scan Activity view in Cloud Security > File Security now supports filtering by Cloud Provider, Account, and Region (added in the GCP v2.3.1 and Azure v2.5.2 templates), displays detailed scan error information for failed scans, and tracks scan counts grouped by Bucket and Scan Type. Event forwarding throughput was also improved for faster scan result availability, especially for high-volume scans.

Narrow down scan activity to a specific GCP account and region to investigate scan errors in a targeted bucket.

> 📍 In the Trend Vision One console, go to Cloud Security › File Security, open Scan Activity, then use the Cloud Provider, Account, and Region filters to scope results,

and select a scan entry to view detailed scan error information.

Narrow down scan activity to a specific Azure account and region to investigate scan errors for a particular storage workload.

> 📍 In Trend Vision One, go to Cloud Security › File Security, open the Scan Activity view, then use the filter controls to select Cloud Provider: Azure, your target Account, and the desired Region. Review the error detail panel for any failed scans, and check the Bucket and Scan Type grouping for scan counts.

— Names filters and fields but mechanism of throughput fix is vague

File Security Storage has released temp… File Security Storage has released temp…

---

03 **Workbench alert and Case Management in Mobile app** NEW

68

The TrendAI Vision One Mobile app now supports reviewing Workbench alerts with filtering by time range and display of severity and current status, opening a Case Management case directly from an alert, and updating case status from the app with changes reflected in the console.

Triage an incoming Workbench alert and escalate it to Case Management without needing console access.

> 📍 In the TrendAI Vision One Mobile app, go to Workbench Alerts › filter by time range › select an alert › tap Open Case Management case › set case status.

— Clear workflow and UI path, but no API or config names given

TrendAI Vision One Mobile app support f…

File Security Storage has released template version 2.3.1 for Google Cloud (2026-10-01

BLOG ↗ STABLE

File Security Storage template v2.3.1 for Google Cloud adds scan activity filters by Cloud Provider, Account, Region, and grouped scan count tracking.

└──▷ **HOW TO FIND IT**

Narrow down scan activity to a specific GCP account and region to investigate scan errors in a targeted bucket.

> 📍 In the Trend Vision One console, go to Cloud Security › File Security, open Scan Activity, then use the Cloud Provider, Account, and Region filters to scope results, and select a scan entry to view detailed scan error information.

Adds detailed scan error information to the Scan Activity view.

Adds scan count tracking grouped by Bucket and Scan Type in the Scan Activity view.

Improves event forwarding throughput for faster scan result availability, especially for high-volume scans.

`TrendAI Vision One Mobile app support for managing Workbench alerts (2026-10-01)`

BLOG ↗ LATEST STABLE

TrendAI Vision One Mobile app adds Workbench alert review, Case Management creation, and case status updates.

└──▷ **HOW TO FIND IT**

Triage an incoming Workbench alert and escalate it to Case Management without needing console access.

📍 In the TrendAI Vision One Mobile app, go to Workbench Alerts › filter by time range › select an alert › tap Open Case Management case › set case status.

Adds Workbench alert management to the TrendAI Vision One Mobile app, with filtering by time range and display of severity and current status for each alert.

Enables opening a Case Management case directly from a Workbench alert in the Mobile app.

Enables updating case status from the TrendAI Vision One Mobile app, with changes reflected in the console.

WAS THIS USEFUL? 👍 👎

Iru

Feedback ⓘ MDM enabled user reporting for Mac NOTES ↗ STABLE RANK

Iru is a device-centric platform that unifies security, IT, and compliance around devices and everything they touch.

Iru surfaces MDM user-channel status in device records, Prism Users category, and the enterprise API.

Adds MDM user-channel enrollment status to the user list on Mac device records.

Exposes MDM user-channel enrollment status in the Prism Users category for bulk reporting.

Exposes MDM user-channel enrollment status via the enterprise API for bulk reporting.

NEW SUPPORTED PLATFORM Safari Extensions management on macOS

NEW SUPPORTED PLATFORM Apple Restrictions Library Item — Siri and Apple Intelligence controls

▾ 3 more releases in this issue · 2026-09-30

> Manage Safari Extensions for Mac NOTES ↗ STABLE
>
> Safari Extensions Library Item now supports macOS Safari Extension management; requires user channel MDM enabled for the target Mac user.

> Managed OS for Apple: Dynamic timeline view NOTES ↗ STABLE
>
> Iru Managed OS for Apple gains a dynamic timeline view showing when updates will be enforced and to which version.



Adds a dynamic timeline view to Managed OS for Apple devices that reflects Library Item settings, showing enforcement deadlines and target OS versions at a glance.

New Apple Restrictions for Siri and Apple Intelligence NOTES ↗ LATEST STABLE

Iru automatically deploys the new restrictions in DDM declarations alongside any existing restrictions deployed using MDM.

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Datadog Stratus Red Team

Feedback ⓘ v2.37.0 NOTES ↗

CODE ↗ RANK

Granular, Actionable Adversary Emulation for the Cloud

> Stratus Red Team added a new AWS persistence technique for suspicious EC2 key pairs and improved the reliability of its S3 ransomware detonation technique against buckets that block SSE-C by default.

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

01 **EC2 suspicious keypair persistence technique** NEW 95

Adds the `aws.persistence.ec2-create-suspicious-keypair` technique, simulating attacker persistence via `ec2:CreateKeyPair` with a short generic key name (`xg1`), preceded by an `ec2:DescribeInstances` recon call filtered by key name. The technique is mapped to MITRE ATT&CK T1098.001 (Account Manipulation: Additional Cloud Credentials) and requires no prerequisite Terraform infrastructure.

Emulate an attacker planting a persistence EC2 key pair with a suspicious name to validate detection of `ec2:CreateKeyPair` with generic key names.

```
$ stratus detonate aws.persistence.ec2-create-suspicious-keypair
```

— Names technique id, API calls, MITRE mapping, and runnable command. v2.37.0

02 **S3 ransomware detonation reliability improvement** IMPROVED 93

Improves the `aws.impact.s3-ransomware-client-side-encryption` technique to allow SSE-C on target buckets before detonation, by calling `PutBucketEncryption` with `BlockedEncryptionTypes` set to `NONE` . This enables `CopyObject` with customer-provided keys to succeed on new buckets that block SSE-C by default.

Emulate client-side S3 ransomware encryption against a fresh bucket (where SSE-C was previously blocked by default) to validate detection of `PutBucketEncryption` and abnormal object overwrite patterns.

```
$ stratus detonate aws.impact.s3-ransomware-client-side-
encryption
```

— Names exact API calls and parameters plus runnable detonation command. v2.37.0

v2.37.0 NOTES ↗ CODE ↗ LATEST STABLE

Stratus Red Team v2.37.0 adds a new AWS EC2 suspicious keypair persistence technique and improves S3 ransomware detonation reliability.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v2.37.0 https://github.com/DataDog/stratus-red-team.git
# already have the repo? check out this version:
$ git checkout v2.37.0
```

└──▷ **TRY IT**

Emulate an attacker planting a persistence EC2 key pair with a suspicious name to validate detection of `ec2:CreateKeyPair` with generic key names.

```
$ stratus detonate aws.persistence.ec2-create-suspicious-keypair
```

Emulate client-side S3 ransomware encryption against a fresh bucket (where SSE-C was previously blocked by default) to validate detection of `PutBucketEncryption` and abnormal object overwrite patterns.

```
$ stratus detonate aws.impact.s3-ransomware-client-side-encryption
```

Adds `aws.persistence.ec2-create-suspicious-keypair` technique, simulating attacker persistence via `ec2:CreateKeyPair` with a short generic name (`xg1`), preceded by an `ec2:DescribeInstances` recon call filtered by key name; mapped to MITRE ATT&CK T1098.001 (Account Manipulation: Additional Cloud Credentials) with no prerequisite Terraform infrastructure.

Improves the `aws.impact.s3-ransomware-client-side-encryption` technique to allow SSE-C on target buckets before detonation by calling `PutBucketEncryption` with `BlockedEncryptionTypes` set to `NONE`, enabling `CopyObject` with customer-provided keys to succeed on new buckets that block SSE-C by default.

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

OpenCTI

Feedback ⓘ 7.260811.0-lts.1 NOTES ↗ RANK

Open Cyber Threat Intelligence Platform

> OpenCTI 7.260811.0-lts.1 removes an external dependency from its map widgets and hardens its container base image for compliance-sensitive deployments.

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

01 **Local PMTiles rendering for map widgets** IMPROVED 45

OpenCTI replaces the external map tile server with local PMTiles rendering, eliminating the outbound dependency previously required for map widgets.

– Explains the change and benefit but no config detail. 7.260811.0-lts.1

02 **FIPS 140-3 validated Docker base image** IMPROVED 25

OpenCTI adopts a FIPS 140-3 validated Docker base image, per the release summary.

– Named compliance standard but no further mechanism or config given. 7.260811.0-lts.1

7.260811.0-lts.1 NOTES ↗ LATEST STABLE

OpenCTI 7.260811.0-lts.1 switches map rendering to local PMTiles and adopts a FIPS 140-3 validated Docker base image.

└──▷ **GET THIS VERSION**

```
$ git clone --branch 7.260811.0-lts.1 https://github.com/OpenCTI-Platform/opencti.git
# already have the repo? check out this version:
$ git checkout 7.260811.0-lts.1
```

Replaces the external map tile server with local PMTiles rendering, eliminating the outbound dependency for map widgets.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

JumpCloud

Feedback ⓘ Release Notes 2022 (2026-10-01) BLOG ↗

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.

> Across nine releases, JumpCloud shipped major platform additions — Device Monitoring and Alerting, a full SaaS Management suite with a Shadow AI Dashboard, an MCP Server for AI client access, JumpCloud Access Requests, and a much-expanded Password Manager — alongside steady growth in MFA, RADIUS, Apple/Windows/Android MDM policies, Asset Management, and two breaking API migrations.

└──▷ **WHAT SHIPPED · 53 FEATURES** most completely described first ? what's the number?

01 **MCP Server for Users** NEW 95

Adds MCP Server for Users (Model Context Protocol) so JumpCloud users can connect AI clients to User Portal capabilities via OAuth sessions. Admins enable it at `Settings > JumpCloud AI` and can set automatic session expiration or revoke sessions manually; users view or revoke their own sessions at `Security > JumpCloud MCP` in the User Portal.

Enable MCP Server for Users so your team can run JumpCloud User Portal tasks from an AI client without switching tools.

📍 In the Admin Portal, go to Settings › JumpCloud AI and toggle on MCP Server for Users. Optionally configure an automatic session expiration window. Users then connect their AI client via OAuth and can view or revoke their own sessions at Security › JumpCloud MCP in the User Portal.

— Exact admin and user navigation paths with OAuth mechanism.

Release Notes 2026 (2026-10-01)

02 **Password Manager admin management and cross-platform builds**

IMPROVED 90

Password Manager gains admin management of shared folder assignments and permissions from the Admin Portal (create/update shared folders, view and assign users or user groups), manual per-folder sync from the desktop app, Cloud Backup as a secure fallback to minimize data loss, a Linux desktop build for Debian/Ubuntu (x86), an ARM build for macOS M-series (M1+) devices with automatic migration from x64 on eligible hardware, an RPM build for Linux x64 Red Hat distributions (e.g. Fedora) with auto-

update, installation and update of the desktop app via command template v2.0.0 on Windows and macOS (removing the need for per-user admin permissions after the first run), and shared folder events synced to Directory Insights in the Admin Portal.

Assign a user group to a newly created shared folder so the whole team gets access without per-user configuration.

> 📍 In the JumpCloud Admin Portal, go to Password Manager › Shared Folders, select or create a folder, then choose `Assign Users or User Groups` and add the target group.

Push a silent install of the Password Manager desktop app to all managed macOS endpoints so users never need to self-install or hold admin rights for future updates.

> 📍 In the JumpCloud Admin Portal, go to Commands, create a new command from the `Install and Update JumpCloud Password Manager` template v.2.0.0, select your macOS device group, and run it.

— Names exact command template and admin steps across releases.

What's New: Password Manager Desktop Ap… | Release Notes 2023 (2026-10-01)

---

03 **Reactivate endpoint moved to POST** BREAKING 90

The deprecated `GET api/systemusers/reactivate/{id}` endpoint now returns a 404 error; it is replaced by `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` accepting `{ activation_email: {email_address} }` in the request body. Any script, automation, or integration must be updated.

Reactivate a user account using the new POST endpoint after removing any existing GET-based automation.

```
$ curl -s -X POST
'https://console.jumpcloud.com/systemusers/reactivate/{id}' \
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json' \
  -d '{ "activation_email": "{email_address}" }'
```

— Exact endpoints, method, body, and runnable example. Release Notes 2024 (2026-10-01)

---

04 **Asset Management enhancements** IMPROVED 90

Asset Management gains an `Asset Manager` role in the Admin Portal providing dedicated access without broader admin access, file upload support via the `Invoice` field under Purchase Details (and custom fields of the File Upload type), `Disk Size` in Hardware Specifications, `Local Device Accounts` on the Asset Detail page under Device

Management, cloning of existing assets (automatically clearing unique fields to prevent duplicates), and Asset Visibility and Asset Acknowledgement in the User Portal — enabled at `Device Management > Asset Management > Settings and Fields > General Settings`, with acknowledgement requests and responses recorded in Asset History and email notifications.

— Names exact fields and enablement path across six additions.

Release Notes 2026 (2026-10-01) | Release Notes 2025 (2026-10-01)

---

05 **Custom Risk Policies under Access Risk** NEW 88

Adds Custom Risk Policies under Access Risk to tailor risk detection for Admin Portal, User Portal, device, and SSO application logins — admins choose monitored risk factors, adjust score weights, set policy precedence, and scope policies to specific user groups or SSO applications. Includes a configurable dormant-application inactivity threshold so the risk factor only fires on re-access after the threshold, not on a user's first sign-in.

Tune dormant-app access risk scoring so newly provisioned apps do not flood analysts with noise on first login.

> 📍 In the Admin Portal, go to Access Risk › Configuration and set the dormant application inactivity threshold. The factor now fires only on re-access after the threshold period, not on a user's first-ever sign-in to an SSO application.

— Names config surface, scope, and tuning example. Release Notes 2026 (2026-10-01)

---

06 **Password Manager usability and capacity enhancements** IMPROVED 85

Password Manager desktop app adds multi-select and item sorting, Download Logs and Keyboard Shortcuts options under Settings, EU region selection before account activation (on the activation page for desktop, pairing page for the browser extension), item storage capacity scaled to 13,000 items with autofill enabled or up to 30,000 without autofill (5,000 items per shared folder), an auto-lock schedule defaulting to 15 minutes of inactivity with a configurable maximum of 1440 minutes, an Auto Lock setting that locks the app whenever the device locks, a Move All items button in shared folders, pagination showing 100 items per page, bulk deletion of multiple folders, archiving with view/delete/restore of archived items, a Copy button in Password History, an enhanced CSV export for the legacy Password Manager to support migration into JumpCloud Vault, and a What's New link under Settings > General.

— Numerous named limits and settings, concrete but no commands.

What's New: Password Manager Desktop Ap… | Release Notes 2024 (2026-10-01)

---

07 **SaaS Management feature set** NEW 85

Launches SaaS Management, discovering and tracking SaaS app usage via the JumpCloud Go browser extension, integrating with existing SSO apps, supporting warning/blocking

access controls, and tracking licensing information; admins can manually add applications for tracking before automatic discovery, and the org-wide JumpCloud Go requirement for unmanaged application discovery was removed (the browser extension alone is now sufficient). Later adds a Shadow AI Dashboard under the renamed JumpCloud AI & SaaS Management for visibility into generative AI shadow IT, adoption, usage by department, and most active users, and SaaS License Management, now generally available, automating license tracking for supported SaaS applications with connectors for cost optimization.

— Broad named feature set across two releases, no exact config steps.

Release Notes 2025 (2026-10-01) Release Notes 2024 (2026-10-01)

---

08 **JumpCloud Go passwordless authentication** IMPROVED 83

JumpCloud Go is a browser extension delivering hardware-protected, phishing-resistant passwordless login using Apple Touch ID and Windows Hello on managed macOS and Windows devices, and is the default MFA method for conditional access policies on SSO apps with verification on every session. JumpCloud added a `User Portal > Security > Multi-Factor Authentication` section to manage Go sessions, automatic session refresh on login/unlock, and automatic device registration for Go on managed Windows, macOS, and Linux devices (admins control eligibility via device exclusion groups, with fallback to manual registration).

— Names UI path and config concept across three releases. Release Notes 2026 (2026-10-01)

Release Notes 2024 (2026-10-01) Release Notes 2023 (2026-10-01)

---

09 **Multi-Tenant Portal admin capabilities** IMPROVED 83

The Multi-Tenant Portal gains an MSP homepage widget showing aggregate reports across all tenant organizations from the last 24 hours with bulk export as JSON or CSV, user and device management (adding new users and devices, exporting lists, and bulk actions), MSP billing visibility showing available/consumed committed user license counts with JumpCloud contract download, and a Global MFA Requirement setting under `Account > Settings` letting Billing admins bulk enforce MFA across all MSP admins in a tenant.

Enforce MFA for all MSP admins across your multi-tenant portal in one step, rather than configuring individual administrator accounts.

> 📍 In the Admin Portal, go to Account › Settings and enable the Global MFA Requirement toggle.

— Named setting with exact toggle location and example. Release Notes 2024 (2026-10-01)

Release Notes 2023 (2026-10-01) Release Notes 2022 (2026-10-01)

---

10 **API filter pipe-escape support** IMPROVED 83

The JumpCloud API now supports escaping the `|` character with `\` inside `in` and `nin` filter operators, enabling pipe characters within search terms, e.g. `GET /systemusers?filter=department:$in:Finance | Accounting|IT`.

Query users belonging to any of several departments that contain a pipe character in their name, using the new pipe-escape in API filter syntax.

```
$ curl -s -X GET 'https://console.jumpcloud.com/api/systemusers?
filter=department:$in:Finance | Accounting|IT' \
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json'
```

— Runnable curl example with exact filter syntax. Release Notes 2024 (2026-10-01)

11 **Push Bombing Mitigation** NEW 80

JumpCloud Protect adds Push Bombing Mitigation, blocking more than one push notification per resource within a sixty-second period, with admin controls in MFA Configurations and blocked events surfaced in Directory Insights.

Protect admin accounts from push bombing attacks by reviewing the default sixty-second block window and tightening concurrent attempt limits in MFA Configurations.

> 📍 In Admin Portal, go to Security › MFA Configurations, locate the Push Bombing Mitigation section, and adjust the maximum concurrent attempts limit or toggle the protection off for specific use cases.

— Mechanism and exact admin path with example steps. Release Notes 2023 (2026-10-01)

12 **Disk encryption condition in Conditional Access Policies** NEW 80

Adds disk encryption as a new device condition in Conditional Access Policies — checking FileVault on macOS, system drive encryption on Windows, and root disk encryption on Linux — so policies can deny access from unencrypted devices.

Deny access to resources from unencrypted devices by adding a disk-encryption condition to a Conditional Access Policy.

> 📍 In the Admin Portal, go to Security › Conditional Access, create or edit a policy, add the device condition 'disk encryption is disabled', set the action to Deny, and assign the policy to the target user group.

— Named per-OS mechanism plus exact admin steps. Release Notes 2022 (2026-10-01)

13 **Remote Assist feature expansion** IMPROVED 80

JumpCloud Remote Assist launched as free remote desktop access for Windows and macOS devices (requires JumpCloud Agent v1.61.0+), with no limits on session time or count. It gained user-switching between accounts during sessions on Windows, a `Ctrl+Alt+Del` command shortcut from the Session Options toolbar, support for Windows server initial login screens (credential entry and user login), separate ARM64 (Apple Silicon) and x86_64 (Intel) packages, an inactivity timer, and automatic detection and termination of unresponsive existing agent instances when an admin initiates a new connection.

— Many named increments but no exact UI paths given. Release Notes 2024 (2026-10-01) Release Notes 2023 (2026-10-01) Release Notes 2022 (2026-10-01)

---

14 **macOS device update and software management policies** NEW

80

Adds the ability to update or force-update a single macOS device from the Admin Portal with configurable update timeframes and user deferral settings, new macOS software management policies to delay or block upgrades to macOS Ventura, and a Managed Login Items policy for macOS 13 Ventura to prevent end users from disabling persistent software such as the JumpCloud Agent.

Block macOS Ventura upgrades fleet-wide while your org validates compatibility with the new OS.

> 📍 In the Admin Portal, go to Device Management › Policies, create a new policy using the macOS software management policy for `Delay or Block MacOS Ventura`, apply it to the target device group, and save.

— Three named policies with exact steps for one. Release Notes 2022 (2026-10-01)

---

15 **Device Monitoring and Alerting** NEW

80

Introduces JumpCloud Device Monitoring and Alerting — monitor device health (availability, software, uptime, disk, battery), policy/command/software management results, directory user addition and privilege elevation events, and custom alerts via command execution monitoring, across Windows, macOS, and Linux endpoints.

— Detailed scope across platforms, no setup path given. Release Notes 2024 (2026-10-01)

---

16 **Patch management policies and reporting** IMPROVED

78

Adds a universal Google Chrome Browser Patch Management policy covering macOS, Windows, and Linux from a single policy, an OS Patch Management Policy Report showing which policies are applied to each device and current compliance status, a Browser Patch Management Policy Report for compliance audit evidence on browser versions, and a Device Patch Report (Windows) in JumpCloud Reports showing per-

device Installed, Pending, and Failed KB status, exportable as CSV with up to a 500-row portal preview.

— Names export format and limit for the newest report. Release Notes 2026 (2026-10-01) Release Notes 2022 (2026-10-01)

17 **Knowledge Base Uploads for AI Assistant** NEW 78

Adds Knowledge Base Uploads for the AI Assistant: upload PDF, TXT, DOCX, and MD files (up to 10 MB each, 25 files per org) into a private org-scoped knowledge base; responses citing uploaded docs attribute the source document.

— Exact file types and limits named, no upload path given.

Release Notes 2026 (2026-10-01)

18 **Dynamic Groups with attribute-based rules** NEW 75

Enables automation of device and user group membership via Dynamic Groups with attribute-based rules, including new Vendor, Public IP Address (device), and Manager (user) attributes.

Automate device group membership for all macOS devices from a specific vendor to apply targeted policies without manual curation.

> 📍 In Admin Portal, go to Device Groups › New Group › enable Dynamic, add a rule for Vendor equals the target vendor name, then optionally enable 'Review membership changes before they take effect'.

— Named attributes plus a concrete setup example. Release Notes 2023 (2026-10-01)

19 **Windows MDM policy additions** NEW 75

Adds a Windows MDM policy to configure Simple Certificate Enrollment Protocol (SCEP), a new Windows MDM Policy Management framework using Configuration Service Providers (CSPs) with six policies (Windows Wi-Fi Configuration, Windows VPN, Install Certificate, Bluetooth Configuration, Control Policy Conflict — enabled by default, and Windows Notification Service — enabled by default), and three Windows Personalization policies (Taskbar Customization, Screen Saver Configuration, and Desktop and Lock Screen Settings).

— Names all nine policies, no configuration steps. Release Notes 2025 (2026-10-01) Release Notes 2024 (2026-10-01)

20 **MFA factor and enrollment additions in JumpCloud Protect** NEW 73

JumpCloud Protect/MFA gains Time-based One-time Password (TOTP) as a supported factor for LDAP applications, Duo Universal Prompt support, a split of WebAuthn into

separate Security Keys and Device credential types for enrollment, MFA enabled by default for all new admin accounts, push notification approval and denial from the device lock screen (long-press on iOS, expand on Android), the ability to allow users to reset passwords from the User Portal when MFA is enforced but not yet enrolled, and User Group Exclusion from Unified MFA letting specific groups use TOTP only instead of Push.

Exclude a remote-region user group from Push MFA enforcement so those users can authenticate with TOTP only.

> 📍 In the Admin Portal, go to JumpCloud Protect › Unified MFA Settings › User Group Exclusions, select the group of users in regions where Push enrollment is unavailable, and save.

— Several named factor/policy additions, no deep mechanism for most.

Release Notes 2025 (2026-10-01) Release Notes 2024 (2026-10-01) Release Notes 2023 (2026-10-01) Release Notes 2022 (2026-10-01)

---

21 **Android management policies and enrollment** IMPROVED

73

Adds Android zero-touch enrollment for fully managed, dedicated, and company-owned Android devices with a work profile, 7 new Android EMM policies for fully managed and dedicated devices including Factory Reset Protection, Kiosk Mode, and System Updates, and new Android policies for Display Settings, Autofill, Work Account authentication, Default App and Intent Handling, and enhanced Bluetooth Restrictions (including outbound file sharing and personal-profile Bluetooth controls on company-owned devices).

— Many named policies, no configuration steps. Release Notes 2026 (2026-10-01) Release Notes 2023 (2026-10-01)

---

22 **Apple MDM enrollment and policy additions** NEW

73

Supports BYOD enrollment of iOS/iPadOS 18+ devices via Account-Driven User Enrollment (ADUE), now in general availability; adds Apple Business Manager as a new service discovery method for Account-driven Enrollment; adds two MDM policies to restrict Apple Intelligence features on iOS/iPadOS 18.1 and macOS 15.1 Sequoia devices; and adds App Settings Privacy policies — a user-level `macOS App Settings Privacy` policy (macOS 27+, supervised Macs) and a device-level `iOS and iPadOS App Settings Privacy` policy (iOS/iPadOS 27+) — to recommend privacy permission defaults for Accessibility, Bluetooth, Camera, Dictation, Local Network, Location, Location Accuracy, and Microphone.

— Several named Apple MDM surfaces, no admin steps. Release Notes 2026 (2026-10-01) Release Notes 2025 (2026-10-01) Release Notes 2024 (2026-10-01)

---

23 **Customer Portal and support case management** IMPROVED

70

Adds JumpCloud Case Portal to centralize support cases and ideas from all admins in a filterable, clickable list, and real-time Live Chat in the Admin Portal for Premium Support customers (replacing chat on the JumpCloud Support site). The Customer Portal later gains sortable columns for `Last Modified Date`, `Account`, and `Requester`, attachment upload and ticket editing on the case page, and MTP admin support to access, view, and create support cases for all tenant organizations.

— Several named portal capabilities, no exact navigation. Release Notes 2025 (2026-10-01) Release Notes 2022 (2026-10-01)

---

24 **Dynamic Groups filter operators changed to $lte/$gte** BREAKING

70

Dynamic Groups `memberQuery` API filters now support `$lte` and `$gte` operators, replacing the deprecated `$le` and `$ge` operators, which API requests must stop using.

— Exact operator names given, no migration example. Release Notes 2024 (2026-10-01)

---

25 **Private Repository enhancements** IMPROVED

70

The JumpCloud Private Repository adds IPA file support for uploading and deploying iOS and iPadOS app packages, and the ability to update the binary of an existing custom application via `Update Version` on the application's `Details` tab, including exit-code confirmation for Windows EXE updates.

— Named UI control and file types, no full workflow. Release Notes 2026 (2026-10-01) Release Notes 2025 (2026-10-01)

---

26 **Windows App Catalog** NEW

68

Launches the JumpCloud App Catalog for Windows with 10 pre-packaged apps (1Password, Adobe Acrobat Reader DC, Chrome, Firefox, Google Drive, OneDrive, OpenVPN, Slack, Webex, Zoom) and auto-update support.

— Names all ten apps and auto-update, no deployment steps.

Release Notes 2024 (2026-10-01)

---

27 **RADIUS authentication enhancements** NEW

65

JumpCloud RADIUS gains certificate (passwordless) based authentication supporting any X.509-compliant certificate authority with import of existing certificates, RADIUS authentication using Azure AD as the identity provider without managing users and passwords outside Azure AD, and faster reconnect for EAP connections using a secure cached session credential to skip the full security handshake on reconnect.

— Mechanism described but no setup steps given. Release Notes 2025 (2026-10-01) Release Notes 2022 (2026-10-01)

28 **Commands area enhancements** NEW 65

JumpCloud Commands gains a Command After Agent Install command type so admins can specify enrollment commands to run immediately after the agent installs, a Running column in the commands queue to distinguish queued from actively running commands, Create Custom Command Templates for MSP admins to save and reuse commands across tenant organizations, and ad hoc command execution on devices directly from the Multi-Tenant Portal and Admin Portal.

— Four named additions, no exact navigation given. Release Notes 2023 (2026-10-01) Release Notes 2022 (2026-10-01)

29 **User Portal application organization** IMPROVED 65

The User Portal Applications area gains All Applications and Favorites tabs with application starring and a responsive search field, and later User Portal Folders letting end users organize assigned applications into private personal folders on the All Applications page (invisible to other users and admins).

— Named UI areas, no exact steps. Release Notes 2026 (2026-10-01) Release Notes 2023 (2026-10-01)

30 **Directory Insights filter field expansion** IMPROVED 65

Expands Directory Insights' Application Name filter into Application Name, Application Display Name, and Application Display Label, and Resource Name into Resource Name, Resource Display Name, and Resource Display Label.

— Names all six filter fields, no usage example. Release Notes 2025 (2026-10-01)

31 **LDAP TLS cipher suite restrictions** BREAKING 65

LDAP TLS no longer accepts connections using CBC-mode or SHA-1/SHA-256 integrity cipher suites, including RSA and ECDHE key exchange variants; only five GCM-based cipher suites are now permitted.

— Specifies cipher classes and count but not the five suite names. Release Notes 2025 (2026-10-01)

32 **AI Gateway Dashboard** NEW 65

Adds an AI Gateway Dashboard tab with org-wide MCP server usage metrics, tool call volume, error rates, trend charts, and per-server drill-down.

— Names metrics shown, no navigation detail. Release Notes 2026 (2026-10-01)

33 **Agent OAuth client authentication type setting** NEW 65

Adds a configurable `client authentication type` for agent OAuth credentials (Client secret basic or Client secret post) on an agent's Authentication tab.

— Exact config option and location named. Release Notes 2026 (2026-10-01)

34 **RSS feed subscriptions for release content** NEW 65

Adds Subscribe to Support RSS Feed on the Release Notes and Bug Fixes page for any new Help Center content, Subscribe to Release Notes and Bug Fixes RSS Feed for product release notes, agent release notes, and bug fix reports, Subscribe to Agent Release Notes RSS Feed for agent-specific notes, and Subscribe to Bug Fixes RSS Feed for bug fix content only.

— Names all four feed options verbatim. Subscribe to New Feature and Product Up…

35 **Password Manager .appimage build deprecated** BREAKING 60

The `.appimage` Linux build of the Password Manager desktop app is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

— Exact deprecation date and migration path named.

What's New: Password Manager Desktop Ap…

THINNER COVERAGE BELOW

36 **SSO protocol and connector additions** NEW 55

JumpCloud SSO adds OpenID Connect (OIDC) support for OIDC-capable web applications, a Deel SSO Connector integration, and integration with AWS Verified Access using JumpCloud Go, SAML, or OIDC SSO as a VPN-less solution for remote corporate resource access.

— Names three integrations but no configuration detail. Release Notes 2023 (2026-10-01)

Release Notes 2022 (2026-10-01)

37 **SentinelOne integration via Commands** NEW 55

Adds a SentinelOne integration, enabling installation of the SentinelOne Agent on macOS, Windows, and Linux devices via JumpCloud Commands.

— Names integration and deployment path, no detailed steps.

Release Notes 2022 (2026-10-01)

38 **JumpCloud Password Manager launch** NEW 55

Launches JumpCloud Password Manager with end-to-end encrypted local storage, browser extension auto-fill, secure password sharing, and password generation.

— Describes core capabilities but no setup path. Release Notes 2022 (2026-10-01)

39 **Self-Service Account Provisioning** NEW 55

Adds Self-Service Account Provisioning, letting new users bind their account to JumpCloud-managed macOS and Windows devices directly from the login window, including a new macOS login window with wireless connectivity controls.

— Mechanism named, no admin setup path. Release Notes 2023 (2026-10-01)

40 **MDM Certificate and Token Status Board** NEW 55

Adds an MDM Certificate and Token Status Board to the Admin Portal and Multi-Tenant Portal homepages, showing expiry status for MDM, SSO, and AzureAD tokens and certificates, with an aggregate MSP view.

— Names scope and surfaces, no interaction detail. Release Notes 2023 (2026-10-01)

41 **Identity First Login two-screen flow** NEW 50

Adds Identity First Login, a two-screen flow for the User Portal and SSO applications that separates username entry from password entry, laying groundwork for passwordless and federation workflows.

— Explains purpose but no setup path. Release Notes 2022 (2026-10-01)

42 **Custom Banned Password List in Password Policies** NEW 45

Password Policies gains a Custom Banned Password List setting letting admins add specific words, terms, and phrases to prohibit from user passwords, configured in the Admin Portal under Password Policies.

Block common weak or company-specific terms across your org to strengthen password hygiene without writing regex rules.

📍 In the Admin Portal, navigate to Password Policies and open the Custom Banned Password List setting. Add the specific words, terms, and phrases you want to prohibit from user passwords, then save the policy.

— Known only from a usage example, no feature bullet exists.

Release Notes 2026 (2026-10-01)

43 **AI Commands Builder GA** NEW 45

Introduces AI Commands Builder, now generally available, enabling natural-language creation and refinement of commands for Windows, macOS, and Linux devices within the Admin Portal.

— States capability and GA status, no usage detail. Release Notes 2025 (2026-10-01)

44 **Background Tools remote command line and file transfer** NEW 45

Adds Background Tools remote command line and remote file transfer capabilities, letting admins access end-user devices and transfer files without disrupting the user.

– Describes behaviour, no UI path or command. Release Notes 2023 (2026-10-01)

45 **Password Date column on Users page** NEW 45

Adds Password Date (the last time a user's password was set) as a viewable column on the Users page in the Admin Portal.

– Thin, single-column addition with exact location. Release Notes 2023 (2026-10-01)

46 **Admin Portal navigation and onboarding updates** IMPROVED 45

Adds a `Cmd/Ctrl + K` keyboard shortcut to the Admin Portal for fast cross-area navigation and search, and renames the Discover page to Get Started, featuring personalized onboarding suggestions and guided support.

– Two thin UX tweaks from the same release. Release Notes 2024 (2026-10-01)

47 **Custom Admin Roles GA** NEW 45

Releases Custom Admin Roles, now generally available for all direct organizations, allowing admins to tailor roles based on specific responsibilities.

– States GA and purpose only, no mechanism. Release Notes 2025 (2026-10-01)

48 **Service Accounts for APIs** NEW 45

Introduces Service Accounts for APIs that are not tied to individual Admin accounts, improving the security and reliability of integrations.

– Describes benefit, no setup detail. Release Notes 2025 (2026-10-01)

49 **PAM Jump Server install, backup, and updates** NEW 40

JumpCloud PAM adds a Jump Server component, including installation support for the jump server, credential backup configuration to protect stored privileged credentials, and an update capability to keep the jump server current.

– Names the capability but no config detail or steps. product docs

50 **Linux platform support additions** NEW 40

Adds JumpCloud agent support for Linux Fedora 37 and a Linux Forbidden Services policy to remove support for unnecessary service types across a Linux fleet.

– Two thin platform additions from the same release. Release Notes 2022 (2026-10-01)

51 **JumpCloud MCP Server GA** NEW 35

Launches JumpCloud MCP Server, generally available, connecting compatible AI tools and code editors to JumpCloud via the Model Context Protocol.

— Only described in the release summary, no mechanism or setup steps.

Release Notes 2025 (2026-10-01)

52 **LDAP source IP tracking** IMPROVED 30

Adds source IP tracking for incoming LDAP requests for enhanced security and traceability.

— One-line addition with no further detail. Release Notes 2025 (2026-10-01)

53 **Access Posture security management capability** NEW 20

JumpCloud adds Access Posture, a new security management capability for evaluating device and user access standing, with a dedicated Get Started guide under JumpCloud's Security Management category.

— Only a name and doc link, no mechanism given. product docs

└──▷ ALSO FROM THESE RELEASES

Configure an Access Requests approval flow with a JIRA webhook so a ticket is auto-created whenever a user submits an access request.

📍 In the Admin Portal, go to Access Requests › Configure Approval Flows, create a flow assigning specific admins as approvers, then under Webhooks add your JIRA webhook URL to receive real-time notifications on new submissions.

└──▷ BREAKING ON UPGRADE

! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; replace it with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `{ activation_email: {email_address} }` in any script, automation, or integration.

! The `$le` and `$ge` filter operators for Dynamic Groups `memberQuery` API filters are deprecated; API requests must use `$lte` and `$gte` instead.

! LDAP TLS no longer accepts connections using CBC-mode or SHA-1/SHA-256 integrity cipher suites (including RSA and ECDHE key exchange variants); only five GCM-based suites are now permitted.

! The `.appimage` Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

Release Notes 2022 (2026-10-01) BLOG ↗ STABLE

JumpCloud 2022 adds certificate-based RADIUS auth, TOTP for LDAP, OIDC SSO, Password Manager, Remote Assist, and a Linux Forbidden Services policy.

└──▷ HOW TO FIND IT

Block macOS Ventura upgrades fleet-wide while your org validates compatibility with the new OS.

📍 In the Admin Portal, go to Device Management › Policies, create a new policy using the macOS software management policy for `Delay or Block MacOS Ventura`, apply it to the target device group, and save.

Deny access to resources from unencrypted devices by adding a disk-encryption condition to a Conditional Access Policy.

📍 In the Admin Portal, go to Security › Conditional Access, create or edit a policy, add the device condition 'disk encryption is disabled', set the action to Deny, and assign the policy to the target user group.

Adds `Command After Agent Install` command type so admins can specify enrollment commands to run immediately after the JumpCloud agent is installed on new devices.

Adds a `Running` column to the commands queue to distinguish commands waiting in queue from those actively running.

Adds certificate (passwordless) based authentication to JumpCloud RADIUS, supporting any X.509-compliant certificate authority — organizations can import existing certificates for RADIUS authentication.

Adds Time-based One-time Password (TOTP) as a supported MFA factor for LDAP applications, alongside JumpCloud Protect push notifications.

Adds MSP multi-tenant homepage widget showing aggregate reports across all tenant organizations available in the last 24 hours, with bulk export as JSON or CSV.

`+18 more`

`Release Notes 2023 (2026-10-01)` `BLOG ↗` `STABLE`

JumpCloud 2023 adds passwordless Go auth, Android zero-touch enrollment, remote Background Tools, dynamic groups, and self-service device provisioning.

└──▷ HOW TO FIND IT

Protect admin accounts from push bombing attacks by reviewing the default sixty-second block window and tightening concurrent attempt limits in MFA Configurations.

📍 In Admin Portal, go to Security › MFA Configurations, locate the Push Bombing Mitigation section, and adjust the maximum concurrent attempts limit or toggle the protection off for specific use cases.

Automate device group membership for all macOS devices from a specific vendor to apply targeted policies without manual curation.

📍 In Admin Portal, go to Device Groups › New Group › enable Dynamic, add a rule for Vendor equals the target vendor name, then optionally enable 'Review membership

changes before they take effect'.

Adds `JumpCloud Go` browser extension for hardware-protected, phishing-resistant passwordless login using Apple Touch ID and Windows Hello on managed macOS and Windows devices.

Adds `JumpCloud Go` as the default MFA method for conditional access policies on SSO apps, with user and device verification on every application session.

Supports Android zero-touch enrollment for fully managed, dedicated, and company-owned Android devices with a work profile.

Adds Background Tools remote command line and remote file transfer capabilities, letting admins access end-user devices and transfer files without disrupting the user.

Adds Self-Service Account Provisioning, letting new users bind their account to JumpCloud-managed macOS and Windows devices directly from the login window, including a new macOS login window with wireless connectivity controls.

+21 more

Release Notes 2024 (2026-10-01) BLOG ↗ STABLE

JumpCloud 2024 adds Device Monitoring & Alerting, Windows App Catalog, SaaS Management, CSP-based MDM policies, and multi-tenant MFA enforcement.

└──▷ **TRY IT**

Query users belonging to any of several departments that contain a pipe character in their name, using the new pipe-escape in API filter syntax.

```
$ curl -s -X GET 'https://console.jumpcloud.com/api/systemusers?
filter=department:$in:Finance | Accounting|IT' \
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json'
```

Reactivate a user account using the new POST endpoint after removing any existing GET-based automation.

```
$ curl -s -X POST
'https://console.jumpcloud.com/systemusers/reactivate/{id}' \
  -H 'x-api-key: <your-api-key>' \
  -H 'Content-Type: application/json' \
  -d '{ "activation_email": "{email_address}" }'
```

Enforce MFA for all MSP admins across your multi-tenant portal in one step, rather than configuring individual administrator accounts.

📍 In the Admin Portal, go to Account › Settings and enable the `Global MFA Requirement` toggle.

Adds `GET /systemusers?filter=department:$in:Finance | Accounting|IT` pipe-escape support — the `|` character can now be escaped with `\` inside `in` and `nin` API filter operators, enabling pipe characters within search terms.

Adds `$lte` and `$gte` filter operators for Dynamic Groups `memberQuery` filters via the API, replacing the deprecated `$le` and `$ge` operators.

Replaces the deprecated `GET api/systemusers/reactivate/{id}` endpoint with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` accepting `{ activation_email: {email_address} }` in the request body.

Introduces JumpCloud Device Monitoring and Alerting — monitor device health (availability, software, uptime, disk, battery), policy/command/software management results, directory user addition and privilege elevation events, and custom alerts via command execution monitoring, across Windows, macOS, and Linux endpoints.

Launches the JumpCloud App Catalog for Windows with 10 pre-packaged apps (1Password, Adobe Acrobat Reader DC, Chrome, Firefox, Google Drive, OneDrive, OpenVPN, Slack, Webex, Zoom) and auto-update support.

`+18 more`

└──▷ **BREAKING ON UPGRADE**

! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; replace it with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `{ activation_email: {email_address} }` in any script, automation, or integration.

! The `$le` and `$ge` filter operators for Dynamic Groups `memberQuery` API filters are deprecated; API requests must use `$lte` and `$gte` instead.

`Release Notes 2025 (2026-10-01)` **BLOG ↗** **STABLE**

JumpCloud: Launches JumpCloud MCP Server GA, connecting compatible AI tools and code editors to JumpCloud via the Model Context Protocol.

└──▷ **HOW TO FIND IT**

Configure an Access Requests approval flow with a JIRA webhook so a ticket is auto-created whenever a user submits an access request.

📍 In the Admin Portal, go to Access Requests › Configure Approval Flows, create a flow assigning specific admins as approvers, then under Webhooks add your JIRA webhook URL to receive real-time notifications on new submissions.

Exclude a remote-region user group from Push MFA enforcement so those users can authenticate with TOTP only.

📍 In the Admin Portal, go to JumpCloud Protect › Unified MFA Settings › User Group Exclusions, select the group of users in regions where Push enrollment is unavailable, and save.

Introduces JumpCloud Access Requests, enabling approval flows, access request management, and webhook integration with ticketing systems such as JIRA.

Adds Shadow AI Dashboard under the renamed JumpCloud AI & SaaS Management for visibility into generative AI shadow IT, adoption, usage by department, and most active users.

Releases Custom Admin Roles GA for all direct organizations, allowing admins to tailor roles based on specific responsibilities.

Introduces Service Accounts for APIs that are not tied to individual Admin accounts, improving security and reliability of integrations.

Adds `Asset Manager` role in the Admin Portal, providing dedicated access to Asset Management without granting broader admin access.

+15 more

└──▷ **BREAKING ON UPGRADE**

! LDAP TLS no longer accepts connections using CBC-mode or SHA-1/SHA-256 integrity cipher suites (including RSA and ECDHE key exchange variants); only five GCM-based suites are now permitted.

`Release Notes 2026 (2026-10-01)` **BLOG ↗** **STABLE**

JumpCloud's October 2026 release adds MCP Server for Users, Custom Risk Policies, a Patch Management Dashboard, AI knowledge-base uploads, and more.

└──▷ **HOW TO FIND IT**

Enable MCP Server for Users so your team can run JumpCloud User Portal tasks from an AI client without switching tools.

📍 In the Admin Portal, go to Settings › JumpCloud AI and toggle on `MCP Server for Users`. Optionally configure an automatic session expiration window. Users then

connect their AI client via OAuth and can view or revoke their own sessions at Security › JumpCloud MCP in the User Portal.

Block common weak or company-specific terms across your org to strengthen password hygiene without writing regex rules.

📍 In the Admin Portal, navigate to Password Policies and open the Custom Banned Password List setting. Add the specific words, terms, and phrases you want to prohibit from user passwords, then save the policy.

Tune dormant-app access risk scoring so newly provisioned apps do not flood analysts with noise on first login.

📍 In the Admin Portal, go to Access Risk › Configuration and set the dormant application inactivity threshold. The factor now fires only on re-access after the threshold period, not on a user's first-ever sign-in to an SSO application.

Adds `MCP Server for Users` (Model Context Protocol) so JumpCloud users can connect AI clients to User Portal capabilities via OAuth sessions; admins enable it at `Settings > JumpCloud AI` and can set automatic session expiration or revoke sessions manually.

Adds `Custom Risk Policies` under Access Risk to tailor risk detection for Admin Portal, User Portal, device, and SSO application logins — choose monitored risk factors, adjust score weights, set policy precedence, and scope policies to specific user groups or SSO applications.

Adds `App Settings Privacy` policies for Apple MDM: a user-level `macOS App Settings Privacy` policy (macOS 27+, supervised Macs) and a device-level `iOS and iPadOS App Settings Privacy` policy (iOS/iPadOS 27+) to recommend privacy permission defaults for Accessibility, Bluetooth, Camera, Dictation, Local Network, Location, Location Accuracy, and Microphone.

Adds `User Portal Folders` so end users can organise assigned applications into private personal folders on the `All Applications` page; folders are invisible to other users and admins.

Adds `Asset Visibility` and `Asset Acknowledgement` in the User Portal, enabled at `Device Management > Asset Management > Settings and Fields > General Settings`; acknowledgement requests and responses are recorded in `Asset History` with email notifications.

`+7 more`

`Subscribe to New Feature and Product Update Announcements (2026-10-01)` `BLOG ↗`

`STABLE`

JumpCloud adds RSS feed subscriptions for release notes, agent updates, and bug fix announcements.

Adds `Subscribe to Support RSS Feed` option on the Release Notes and Bug Fixes page to receive notifications for any new Help Center content.

Adds `Subscribe to Release Notes and Bug Fixes RSS Feed` option to receive product release notes, agent release notes, and bug fix reports.

Adds `Subscribe to Agent Release Notes RSS Feed` option to receive agent-specific release note notifications.

Adds `Subscribe to Bug Fixes RSS Feed` option to receive bug fix content notifications only.

`What's New: Password Manager Desktop App (2026-10-01)` `BLOG ↗` **LATEST**

STABLE

JumpCloud Password Manager Desktop App gains EU region support, 30,000-item capacity, ARM/RPM builds, and shared-folder admin controls.

└──▷ **HOW TO FIND IT**

Assign a user group to a newly created shared folder so the whole team gets access without per-user configuration.

> 📍 In the JumpCloud Admin Portal, go to Password Manager › Shared Folders, select or create a folder, then choose `Assign Users or User Groups` and add the target group.

Push a silent install of the Password Manager desktop app to all managed macOS endpoints so users never need to self-install or hold admin rights for future updates.

> 📍 In the JumpCloud Admin Portal, go to Commands, create a new command from the `Install and Update JumpCloud Password Manager` template v.2.0.0, select your macOS device group, and run it.

Supports EU region selection before account activation — available on the activation page for the desktop app and on the pairing page for the browser extension.

Scales item storage capacity to 13,000 items with autofill enabled, or up to 30,000 items without autofill; one shared folder can hold up to 5,000 items.

Introduces an auto-lock schedule with a default of 15 minutes of inactivity and a configurable maximum of 1440 minutes (24 hours).

Adds a `Move All items` button in shared folders to relocate all items from a folder in a single action.

Paginates the items list, displaying 100 items per page.

`+11 more`

> └──▷ **BREAKING ON UPGRADE**
>
> ! The `.appimage` Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

WAS THIS USEFUL? 👍 👎

Keycloak

Feedback ⓘ Keycloak 26.8.0 released (2026-10-01) BLOG ↗

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 ships multi-cluster v2 stateless deployments that replace the now-deprecated multi-site v1, promotes the SCIM API, OID4VCI issuance, Client Admin API v2 and parameterized scopes toward general availability, and adds OAuth token-exchange delegation scopes alongside new OID4VP verifier, SD-JWT mapper and Shared Signals Framework capabilities.

└──▷ **WHAT SHIPPED · 13 FEATURES** most completely described first ? what's the number?

01 Multi-cluster v2 stateless mode replaces v1

BREAKING

93

`--features=stateless` runs multi-cluster v2 deployments without an external Infinispan cluster, storing session data in the database instead; a new deployment guide covers bare-metal and VM environments alongside the existing Kubernetes guide. Multi-cluster v1 (the multi-site feature) is deprecated and will be removed in a future major release, with `--features=stateless` as the recommended replacement.

Start Keycloak in multi-cluster v2 stateless mode to connect clusters without an external Infinispan deployment.

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

— Names exact flag, storage mechanism, and deprecation/migration path.

Keycloak 26.8.0 released (2026-10-01)

02 **Delegation scopes for token exchange** NEW 87

A new `delegation:client:<client-id>` parameterized scope enables OAuth consent-based token exchange delegation, producing tokens with an `act` claim identifying the delegated client as the actor. `delegation:user` and `delegation:client` client scopes are auto-created as Optional scopes in all realms, with delegation authorization controlled through Fine-Grained Admin Permissions V2 using `delegate` and `delegate-members` scopes. A new client policy executor restricts the `may_act` claim in access tokens, giving per-client control over which clients can participate in delegation.

— Names scopes, claim and executor but no walkthrough example.

Keycloak 26.8.0 released (2026-10-01)

03 **OID4VCI credential issuance promoted to preview** IMPROVED 86

`--features=preview` or `--features=oid4vc-vci` activates OID4VCI verifiable credential issuance (promoted from experimental to preview), adding credential revocation on refresh-token revocation and a new Application Initiated Action for in-session credential requests. An experimental `oid4vc-mdoc` feature flag adds support for the mdoc credential format, and both flags can be enabled together (`--features=oid4vc-vci,oid4vc-mdoc`).

Enable OID4VCI verifiable credential issuance and the experimental mdoc format in a single startup flag.

```
$ bin/kc.sh start --features=oid4vc-vci,oid4vc-mdoc
```

— Runnable flag combination given with named sub-capabilities.

Keycloak 26.8.0 released (2026-10-01)

04 **New client policy executors for hostname and mapper restrictions**

NEW 78

The `secure-client-node-hostname` client policy executor validates cluster node registration hostnames against administrator-configured regex patterns, protecting against SSRF via the legacy adapter endpoint `/clients-managements/register-node`. The `allowed-protocol-mappers` executor restricts which protocol mapper types can be created or updated through Admin REST API protocol mapper endpoints.

— Both executors and their protected endpoints are named.

Keycloak 26.8.0 released (2026-10-01)

05 **Client Admin API v2 promoted to preview** IMPROVED 73

`--features=preview` or `--features=client-admin-api:v2` activates the Client Admin API v2 (promoted to preview), providing strict validation, declarative configuration, and an accurate OpenAPI spec for OIDC and SAML clients.

— Flag named but no worked example of the new API. Keycloak 26.8.0 released (2026-10-01)

06 **OID4VP verifier support for wallet credential presentation**

NEW

68

Experimental OID4VP verifier support enables authentication flows where users present verifiable credentials from digital wallets, supporting cross-device presentation flows and `direct_post.jwt` encrypted response mode. New SD-JWT User Attribute and Session mappers extract claims from verifiable credentials presented via OID4VP.

— Mechanism and mappers named, no enabling flag given.

Keycloak 26.8.0 released (2026-10-01)

07 **Shared Signals Framework event revisions** BREAKING

64

The experimental Shared Signals Framework (SSF) support adds RISC `account-disabled` and `account-enabled` event types. The SSF event structure has been revised for better alignment with CAEP and RISC specifications, so existing consumers should review the updated payload shapes; the admin event store also no longer receives unvalidated SSF payloads, preventing PII leakage.

— New event types and structural/security change named, no migration example.

Keycloak 26.8.0 released (2026-10-01)

08 **Impersonation details in token lifecycle events** IMPROVED

63

Token lifecycle events (`CODE_TO_TOKEN` , `REFRESH_TOKEN` , and others) now include `impersonator` and `impersonator_id` details, and access tokens and ID tokens issued from impersonation sessions include the `act` claim (RFC 8693 Section 4.1).

— Names event types and claim spec, no example given.

Keycloak 26.8.0 released (2026-10-01)

09 **Parameterized scopes promoted to preview** IMPROVED

60

Parameterized scopes (formerly dynamic scopes) are promoted from experimental to preview, allowing clients to pass a parameter value with the scope name (e.g. `project:12345`) in OAuth 2.0 authorization requests.

— Example scope format given, no runnable request shown.

Keycloak 26.8.0 released (2026-10-01)

THINNER COVERAGE BELOW

10 **SCIM API promoted to supported** IMPROVED

59

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

– Lists additions but no endpoint or config example.

Keycloak 26.8.0 released (2026-10-01)

---

11 **Invite-user workflow step** NEW 54

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

– Describes behaviour, no config example shown. Keycloak 26.8.0 released (2026-10-01)

---

12 **Keycloak Operator client custom resources promoted to preview**

IMPROVED 54

`KeycloakOIDCClient` and `KeycloakSAMLClient` Operator custom resources are promoted to preview, enabling declarative client management via the Keycloak Operator.

– Names the CRDs but no manifest example. Keycloak 26.8.0 released (2026-10-01)

---

13 **Client Secret Rotation promoted to supported** IMPROVED 52

Client Secret Rotation is promoted from preview to supported, allowing confidential clients to keep up to two concurrently active secrets during rotation via client policies.

– States concrete limit but no policy config example.

Keycloak 26.8.0 released (2026-10-01)

└──▷ **BREAKING ON UPGRADE**

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

! The Shared Signals Framework event structure has been revised for better alignment with CAEP and RISC specifications; existing consumers of SSF events should review the updated payload shapes.

! The admin event store no longer receives unvalidated SSF payloads to prevent PII leakage.

> Keycloak 26.8.0 released (2026-10-01) BLOG ↗ LATEST STABLE
>
> Keycloak 26.8 adds supported SCIM API and multi-cluster stateless mode, OID4VCI/OID4VP credentials, and token exchange delegation for AI agents.
>
> └──▷ **TRY IT**
>
> Start Keycloak in multi-cluster v2 stateless mode to connect clusters without an external Infinispan deployment.

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

Enable OID4VCI verifiable credential issuance and the experimental mdoc format in a single startup flag.

```
$ bin/kc.sh start --features=oid4vc-vci,oid4vc-mdoc
```

Enables `--features=stateless` to run multi-cluster v2 deployments without an external Infinispan cluster, storing session data in the database instead.

Enables `--features=preview` or `--features=oid4vc-vci` to activate OID4VCI verifiable credential issuance (promoted from experimental to preview), with credential revocation on refresh-token revocation and a new Application Initiated Action for in-session credential requests.

Adds experimental `oid4vc-mdoc` feature flag for mdoc credential format support.

Enables `--features=preview` or `--features=client-admin-api:v2` to activate the Client Admin API v2 (promoted to preview), providing strict validation, declarative configuration, and an accurate OpenAPI spec for OIDC and SAML clients.

Promotes the 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.

+14 more

└─▷ **BREAKING ON UPGRADE**

- ! Multi-cluster v1 (the multi-site feature) is deprecated and will be removed in a future major release; the recommended replacement is multi-cluster v2 enabled with `--features=stateless`.
- ! The Shared Signals Framework event structure has been revised for better alignment with CAEP and RISC specifications; existing consumers of SSF events should review the updated payload shapes.
- ! The admin event store no longer receives unvalidated SSF payloads to prevent PII leakage.

WAS THIS USEFUL? 👍 👎

Clerk

Feedback ⓘ Self-serve Directory Sync (2026-09-30) BLOG ↗

RANK

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

IT admins can now self-configure Directory Sync from the Security tab in `<OrganizationProfile />`, removing the need for developer intervention.

NEW INTEGRATION Self-serve Directory Sync via OrganizationProfile

WAS THIS USEFUL? 👍 👎

Nudge Security

Feedback ⓘ

Address sprawling OAuth and browser extension risk with Nudge Security AI agents, now li

NOTES ↗ RANK

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

Nudge Security launches two AI agents — OAuth Grant Risk Analyst and Browser Extension Risk Analyst — for automated SaaS attack surface remediation at scale.

NEW DETECTION Adds the OAuth Grant Risk Analyst AI agent, which reviews new OAuth grants as they are discovered, automatically revokes overly permissive or high-risk access, or nudges the OAuth grantor to remove it, with human-in-the-loop oversight.

NEW DETECTION Adds the Browser Extension Risk Analyst AI agent, which inspects artifacts and metadata behind installed browser extensions, flags malicious, compromised, or misrepresented extensions, and orchestrates disable and uninstall workflows.

AI agents are accessible via `Automations > AI Agents` in the Nudge Security console.

WAS THIS USEFUL? 👍 👎

1Password

Feedback ⓘ 1Password SaaS Manager #1890 (2026-09-29)

BLOG ↗ STABLE RANK

All the latest releases from the 1Password team

Adds Usage export field for applications, granular AI Consumption access controls, deferred user imports with estimated counts, and connected-source team indicators.

Adds `Usage` as a selectable field when exporting application information.

Enables granting access to AI Consumption independently of Spend data for other applications.

Allows admins to defer user imports for newly discovered apps until they are managed, with pending apps showing an estimated user count, improving initial sync performance for very large organizations.

Surfaces an indicator when a team is managed by a connected source so admins know where to make changes.

UPDATED INTEGRATION Microsoft Entra ID cost center mapping via cloud extension attributes

▾ 5 more releases in this issue · 2026-09-29

> 1Password for Linux 8.12.38 (2026-09-29) BLOG ↗ STABLE
>
> 1Password for Linux can now connect to AI agents to approve and fulfill sign-in requests on your behalf.
>
> Connects 1Password to supported AI agents so they can sign in to websites on your behalf, with per-request approval and vault selection from your Private vault.
>
> Adds breadcrumb navigation to the Developer Watchtower page.
>
> Adds programmatic access options for the 1Password CLI and SDKs in Developer Environments, along with an option to copy the environment ID.

> 1Password for Mac 8.12.38 (2026-09-29) BLOG ↗ STABLE
>
> 1Password: Adds `Settings > Autofill > 'Disable macOS Autofill'` option so users can turn off macOS Autofill directly from 1Password preferences.
>
> └──▷ HOW TO FIND IT
>
> Disable macOS system-level Autofill from 1Password when you want to prevent it from filling credentials in native macOS prompts.
>
> 📍 In 1Password, go to Settings › Autofill › `Disable macOS Autofill`.

Expands macOS Autofill to more surfaces, including server connections in Finder, with a confirmation prompt before filling.

└──▷ **BREAKING ON UPGRADE**

! The default Quick Access keyboard shortcut on macOS 27 is changed to Option Command Backslash; any workflow or documentation relying on the previous shortcut will need to be updated.

1Password for Windows 8.12.38 (2026-09-29) BLOG ↗ STABLE

1Password: Adds Trusted Platform Module (TPM) support on by default for the Convenient and Balanced security presets when Unlock using Windows Hello is enabled.

Simplifies the steps to add an account from 1Password.com or by scanning a QR code with 1Password on mobile.

1Password for iOS 8.12.38 (2026-09-29) BLOG ↗ STABLE

Autofill unlocking improved so one Face ID scan unlocks every available account at once.

1Password in the browser 8.12.38 (2026-09-29) BLOG ↗ LATEST STABLE

1Password in the browser now saves logins across split username/password screens and shows which app version the extension is connected to.

Adds save-login prompts for sites that present username and password on separate screens.

Settings now displays whether the browser extension is connected to 1Password 7 or 1Password 8.

WAS THIS USEFUL? 👍 👎

P0 Security

Feedback ⓘ

Agents are redefining sensitive access and P0 is leveraging AI to extend coverage just as

BLOG ↗ RANK

P0 Security delivers runtime access control for AI, built on a proven runtime authorization platform for humans and machines. Discover the agents operating across your environment and the identities, tools and privileges they use.

P0 uses AI-assisted development to accelerate connector authorship, with human review before shipping to customer environments.

AI-assisted connector authoring reduces integration work to roughly 150 lines of code built in under an hour, with human engineer review before release.

NEW INTEGRATION Salesforce connector

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ v4.0.8 NOTES ↗ RANK

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

Adds cross-domain whiteboard asset loading, inline control linking buttons, and custom audit scoring without framework cloning.

└──▷ GET THIS VERSION

```
$ git clone --branch v4.0.8 https://github.com/intuitem/ciso-assistant-community.git
# already have the repo? check out this version:
$ git checkout v4.0.8
```

Enables pulling assets from external domains on the whiteboard.

Adds `create` and `select-existing` buttons directly on linked-object tabs in applied controls, reducing navigation steps when associating controls.

Introduces a new way to set a custom score on an audit without cloning the framework.

NEW COMPLIANCE FRAMEWORK SCF 2026.3 framework

UPDATED COMPLIANCE FRAMEWORK Essential Eight framework

WAS THIS USEFUL? 👍 👎

AGENT

◆ MCP Servers & Tooling

Runlayer

Feedback ⓘ 1.28.911 (2026-09-30) BLOG ↗ RANK

Runlayer is an MCP gateway that enforces identity-mapped permissions and detects threats across the agents and MCP servers employees use.

> Runlayer added Terraform support for deploying its self-hosted Rev decision model and optional OTel Collector and procedures-validator sidecars on ECS, alongside MCP-driven artifact link management and usability improvements to Shadow AI filtering and the Integrations page.

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

01 **Self-hosted Rev decision model in ECS Terraform deployment**

NEW 97

Adds `enable_runlayer_rev` Terraform input to run Rev, Runlayer's self-hosted decision model, as a third container (`runlayer-topic-cpu-rev`) in the topic CPU task, exposing `POST /predict/runlayer-rev` on NLB port 8082 and setting `RUNLAYER_REV_ENDPOINT_URL` and `RUNLAYER_REV_TIMEOUT` on the backend (requires `enable_runlayer_topic_cpu = true`). Also adds `runlayer_rev_image_tag` (must start with `runlayer-rev-guard-v` , e.g. `runlayer-rev-guard-v202609292007`), `runlayer_rev_gunicorn_workers` (range 1–6, each worker loading its own fp32 encoder at ~2.5–2.7 GiB RSS), `runlayer_rev_memory` (must be at least `(workers + 1) * 2560 MiB` to accommodate recycler overlap), `runlayer_rev_cpu_share` (fractional CPU units from the slow pool's remainder; fast share + Rev share must stay below 1 unless an absolute override is set), and `runlayer_rev_timeout` (1–60 seconds, matching operator field `topicCpu.rev.timeoutSeconds`).

Deploy the self-hosted Rev decision model on an m7i.2xlarge with 2 workers, sized to fit alongside the slow and fast containers within the 30720 MiB instance limit.

```hcl
enable_runlayer_rev        = true
enable_runlayer_topic_cpu  = true
runlayer_rev_image_tag     = "runlayer-rev-guard-v202609292007"
runlayer_rev_gunicorn_workers = 2
runlayer_rev_memory        = 8192
runlayer_rev_cpu_share     = 0.20
runlayer_rev_timeout       = 10
```

— Names every Terraform input, range and mechanism involved product docs

02 **OTel Collector sidecar for ECS tasks** NEW 84

Adds an optional OTel Collector sidecar for backend and worker ECS tasks; when enabled it adds a second container receiving telemetry via `localhost:4317`, with `export_endpoint` set to a customer-owned OTLP gRPC endpoint (loopback values are rejected at plan time), while Runlayer-side export is configured separately via `runlayer_obs_otel_*` inputs.

Enable the OTel Collector sidecar and forward telemetry to a customer-owned OTLP gRPC endpoint, while keeping Runlayer-side export configured separately.

```hcl
otel_collector = {
  export_endpoint = "otel-collector.internal:4317"
}
```

— Names the sidecar, port and config keys with an example product docs

03 **Procedures-validator sidecar for serving backend** NEW 80

Adds `procedures_validator` Terraform input for an optional procedures-validator sidecar on the serving backend task, accepting object({ image = string, cpu = optional(number, 128), memory = optional(number, 512) }) with the image required to be explicitly tagged or digest-pinned.

Attach a procedures-validator sidecar to the serving backend, pinned to a specific digest, with custom CPU and memory reservations.

```hcl
procedures_validator = {
  image  = "registry.example.com/procedures-
validator@sha256:abc123"
  cpu    = 256
  memory = 1024
}
```

— Full schema and defaults given with example product docs

THINNER COVERAGE BELOW

04 **Shareable URL-persisted Shadow AI filters** IMPROVED 50

Persists Shadow AI Details table filters in the page URL so filtered views can be shared directly, with Back returning to the originating dashboard tab.

— Describes behaviour but no exact UI path or param name 1.28.911 (2026-09-30)

05 **Collapsed Connected Agent Apps list on Integrations page**

IMPROVED

50

Collapses the Connected Agent Apps list on the Integrations page by default with a count, preventing long page loads in large Slack workspaces.

— Clear UI change but no config or metric given 1.28.911 (2026-09-30)

06 **Artifact custom-link management via MCP** NEW

35

Enables assistants and agents to set, change, remove, and open an artifact by its custom link through Runlayer MCP.

— No specific command or API named 1.28.911 (2026-09-30)

> 1.28.911 (2026-09-30) BLOG ↗ LATEST STABLE
>
> Runlayer 1.28.911 adds artifact custom-link management via MCP and shareable URL-persisted Details filters for Shadow AI.
>
> Enables assistants and agents to set, change, remove, and open an artifact by its custom link through Runlayer MCP.
>
> Persists Shadow AI Details table filters in the page URL so filtered views can be shared directly, with Back returning to the originating dashboard tab.
>
> Collapses the Connected Agent Apps list on the Integrations page by default with a count, preventing long page loads in large Slack workspaces.

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

Operant AI

Feedback ⓘ

Announcing Operant's Coverage for Microsoft Copilot and Every AI Assistant Embedded in M

NOTES ↗ RANK

Operant AI discovers, detects and defends AI applications, agents, MCP servers, APIs and Kubernetes workloads at runtime.

> Operant AI shipped a Microsoft 365 coverage push this window: a Microsoft Purview integration for Copilot observability and data-exposure detection, inline Agent Protector runtime checks for the Agents SDK, label-aware plugin blocking driven by Purview sensitivity labels, third-party assistant blocking on the web, and broader anomaly/jailbreak detection across agent sessions.

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

01 Label-aware plugin blocking via Purview sensitivity labels

NEW 85

Uses existing Microsoft Purview sensitivity labels to block specific AI vendors or plugins from accessing documents based on classification rules. Configured under Policies > Label-Aware Plugin Rules in the Operant console, for example blocking Harvey on documents labeled Highly Confidential – Board, blocking Rogo on documents labeled MNPI – Restricted, and allowing Copilot across all labels while blocking any third-party assistant not on the approved vendor list.

Enforce label-aware plugin blocking so that sensitive documents never reach unapproved third-party AI vendors — without reclassifying any content.

📍 In the Operant console, go to Policies › Label-Aware Plugin Rules, create a rule: Block Harvey on documents labeled Highly Confidential – Board; Block Rogo on documents labeled MNPI – Restricted; Allow Copilot on all labels while blocking any third-party assistant not on the approved vendor list.

— Exact UI path and concrete rule example make this actionable

Announcing Operant's Coverage for Micro…

02 Agent Protector inline protection for M365 Agents SDK NEW

65

Agent Protector integrates into the Microsoft 365 Agents SDK runtime, evaluating each tool invocation, retrieved content, outbound call, and write action inline before it executes. In this inline path it detects indirect prompt injection in retrieved content — including instructions hidden in emails and documents — before it enters an agent's

context, and flags loop behavior anomalies such as iteration counts, retries, and sudden plan changes as signals of agent redirection.

— Explains inline mechanism, no exact config or command

Announcing Operant's Coverage for Micro…

03 **Microsoft Purview integration for Copilot observability** NEW

63

Ingests every Copilot prompt, response, and tool call across all Microsoft 365 Copilot surfaces via a Microsoft Purview integration for detection and audit. Detects sensitive data exposure (PII, PHI, PCI, credentials, source code, MNPI) in Copilot prompts, grounded content, and responses, and flags oversharing when a response draws on content outside the user's normal working set.

— Names the integration and data types but no config surface

Announcing Operant's Coverage for Micro…

THINNER COVERAGE BELOW

04 **Third-party AI assistant blocking in Microsoft 365 web** NEW

48

Adds prompt-level observation, detection, and blocking for third-party assistants such as Harvey and Rogo embedded in Microsoft 365 on the web, blocking individual violating prompts while allowing the session to continue.

— Clear capability but no config or command detail

Announcing Operant's Coverage for Micro…

05 **Anomalous agent activity and cross-session jailbreak detection**

NEW

40

Detects anomalous agent and tool activity — including unusual plugin invocations, retrieval volume spikes, and agents acting outside their declared purpose — and detects jailbreak and policy evasion attempts correlated across sessions and users rather than evaluated per prompt.

— Describes behavior detected but no mechanism or surface named

Announcing Operant's Coverage for Micro…

Announcing Operant's Coverage for Microsoft Copilot and Every AI Assistant Embedded in

NOTES ↗ LATEST STABLE

Operant adds Microsoft 365 AI coverage: Purview-backed Copilot observability, inline Agents SDK protection, and label-aware plugin blocking.

└──▷ HOW TO FIND IT

Enforce label-aware plugin blocking so that sensitive documents never reach unapproved third-party AI vendors — without reclassifying any content.

> 📍 In the Operant console, go to Policies › Label-Aware Plugin Rules, create a rule: Block `Harvey` on documents labeled `Highly Confidential – Board`; Block `Rogo` on documents labeled `MNPI – Restricted`; Allow Copilot on all labels while blocking any third-party assistant not on the approved vendor list.

Adds a Microsoft Purview integration that ingests every Copilot prompt, response, and tool call across all Microsoft 365 Copilot surfaces for detection and audit.

Adds Agent Protector integration into the Microsoft 365 Agents SDK runtime, evaluating each tool invocation, retrieved content, outbound call, and write action inline before it executes.

Adds prompt-level observation, detection, and blocking for third-party assistants (such as Harvey and Rogo) embedded in Microsoft 365 on the web, blocking individual violating prompts while allowing the session to continue.

Adds label-aware plugin blocking that uses existing Microsoft Purview sensitivity labels to block specific AI vendors or plugins from accessing documents based on classification rules.

Detects sensitive data exposure (PII, PHI, PCI, credentials, source code, MNPI) in Copilot prompts, grounded content, and responses via the Purview integration.

+5 more

WAS THIS USEFUL? 👍 👎

AI-Infra-Guard

Feedback ⓘ v4.6.4 NOTES ↗ RANK

A full-stack AI Red Teaming platform securing AI ecosystems via Agent Scan, Skills Scan, MCP scan, AI Infra scan and LLM jailbreak evaluation.

> AI-Infra-Guard added a vendored prompt-injection research toolkit for its Research area.

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

01 **Pikit prompt-injection research toolkit** NEW 45

Vendors `pikit` (NY1024/pikit), a composable prompt-injection research toolkit, placed under `Research/pikit` in the repository.

— Names the exact path and source but no usage detail v4.6.4

v4.6.4 NOTES ↗ LATEST STABLE

Adds pikit, a composable prompt-injection research toolkit, under Research/pikit

└──▷ **GET THIS VERSION**

```
$ git clone --branch v4.6.4 https://github.com/Tencent/AI-Infra-Guard.git
# already have the repo? check out this version:
$ git checkout v4.6.4
```

WAS THIS USEFUL? 👍 👎

NoLabs nono

Feedback ⓘ v0.79.0 NOTES ↗ CODE ↗ RANK

The nono runtime runs AI agents in isolated environments with policy-controlled filesystem, network, and credential access.

> nono's latest window centers on remote agent session management and stronger diagnostics redaction: v0.79.0 adds flags to launch and attach to remote agent sessions and surfaces proxy denials in the CLI, while a new `diagnostics.redaction.extra_env_vars` profile key (later documented in depth) scrubs extra secrets from diagnostics and audit logs.

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

01 Extra environment variable redaction for diagnostics and audit logs

NEW 95

The `diagnostics.redaction.extra_env_vars` profile key redacts additional environment variables from diagnostic output and audit logs, supporting glob syntax (e.g. `ACME_*`, `*_SECRET`) matched case-insensitively against the full variable name using the same matcher as `environment.deny_vars`. Redaction is also derived automatically from `environment.deny_vars` exact-name entries and from `command_policies.credentials`, `network.custom_credentials`, and `credential_routes` `env_var` destinations without a separate declaration. Entries merge additively across profile inheritance so child profiles widen rather than replace the list, each audit record documents its own redaction-policy diff, and removing a secure default requires `[redaction].unsafe_redaction_overrides` in user config since profile-level entries are add-only.

Scrub a deployment credential and a wildcard family of secrets from diagnostics and audit logs when they are passed through the host environment rather than declared in the profile.

yaml

```yaml
diagnostics:
  redaction:
    extra_env_vars:
      - "DEPLOY_TOKEN"
      - "ACME_*"
      - "*_SECRET"
```

— Full mechanism, config keys, and a runnable yaml example given v0.79.0

02 Remote agent session launch and attach NEW 75

`nono run` gains `--remote`, `--agent`, `--workspace`, and `--detached` flags to launch and attach to remote agent sessions, allowing a user to attach interactively to inspect or resume a long-running sandboxed session from another machine, or launch it detached in the background under the sandbox policy.

Attach interactively to a remote agent workspace — useful for inspecting or resuming a long-running sandboxed session from another machine.

```
$ nono run --remote --agent claude --workspace my-project
```

Launch a remote agent session in the background without attaching, then walk away — the session runs detached under the sandbox policy.

```
$ nono run --remote --agent claude --workspace my-project --
detached
```

— Named flags with two runnable example commands v0.79.0

THINNER COVERAGE BELOW

03 **Legacy Claude hook cleanup removed** BREAKING 40

The commit `feat(cli)!: remove legacy Claude hook cleanup` removes legacy Claude hook cleanup code; any setup relying on that automatic cleanup will no longer have it performed on upgrade.

— Named commit but no migration steps provided v0.79.0

04 **Proxy network denial diagnostics in CLI footer** NEW 30

Blocked outbound network calls from the proxy are now rendered in the CLI diagnostic footer, so denials are visible at a glance.

— Described only in prose, no flag or config named v0.79.0

05 **Snap policy group** NEW 10

v0.79.0 introduces a new `Snap` policy group, per the release summary; no further mechanism or configuration detail is provided.

— Name only, no detail given in source v0.79.0

└──▷ BREAKING ON UPGRADE

! Legacy Claude hook cleanup code has been removed (`feat(cli)!: remove legacy Claude hook cleanup`); any setup relying on that automatic cleanup will no longer have it performed on upgrade.

v0.79.0 NOTES ↗ CODE ↗ LATEST STABLE

nono v0.79.0 adds remote agent session launch, proxy denial diagnostics, Snap policy group, and `diagnostics.redaction.extra` _env_vars

└──▷ GET THIS VERSION

```
$ git clone --branch v0.79.0 https://github.com/nolabs-ai/nono.git
# already have the repo? check out this version:
$ git checkout v0.79.0
```

└──▷ TRY IT

Attach interactively to a remote agent workspace — useful for inspecting or resuming a long-running sandboxed session from another machine.

```
$ nono run --remote --agent claude --workspace my-project
```

Launch a remote agent session in the background without attaching, then walk away — the session runs detached under the sandbox policy.

```
$ nono run --remote --agent claude --workspace my-project --detached
```

Adds `--remote`, `--agent`, `--workspace`, and `--detached` flags to `nono run` to launch and attach to remote agent sessions.

Adds `diagnostics.redaction.extra_env_vars` profile key to redact additional environment variables from diagnostic output.

Renders proxy network denials in the CLI diagnostic footer so blocked outbound calls are visible at a glance.

└──▷ BREAKING ON UPGRADE

! Legacy Claude hook cleanup code has been removed (`feat(cli)!: remove legacy Claude hook cleanup`); any setup relying on that automatic cleanup will no longer have it performed on upgrade.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 1, 2026

Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue