

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 23, 2026 · EVERY DAY

EDITIONS **tail** | grep | head | ls | diff | uniq

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 38 changes](#)Do you prefer **scroll**?[▶ // CONTENTS](#) [SHOW](#)

13 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 today. GitGuardian's engine learned ten new secret types and can now test an SMTP credential to see if it

vim ? help

fully works before anyone pages a developer. Sealed Secrets stops

needing a controller restart to pick up new sealing keys or undo hand-edited Secrets. Levo surfaces which API endpoints have no authentication at all.

PROTECT

Tell a live secret from a dead one before opening a ticket

Ten new detectors widen what gets caught, and the SMTP validity checker attempts a real check against the credential rather than just matching a pattern. Validity is what separates a rotation emergency from a stale string in an old commit, and it is the triage step teams otherwise do by hand.

[GitGuardian Detection Engine](#)

PROTECT

Rotate sealing keys without bouncing the controller

The controller reloads sealing keys live and re-reconciles Secrets someone edited directly in the cluster, both without a pod restart. Key rotation stops being a scheduled maintenance event, and a manual `kubectl edit` no longer quietly persists as drift from the sealed source of truth.

[Sealed Secrets](#)

IDENTIFY

See which API endpoints are actually unauthenticated

Authentication becomes a per-endpoint attribute in the inventory, Application Insights and findings, so an unauthenticated route is a filterable property rather than something you infer from traffic. Exportable web application scan files also make a result shareable with a team that does not have a Levo login.

[Levo](#)

PROTECT

Catch unescaped URL path construction in Go at commit time

A new rule flags URL path elements built without escaping — the pattern behind path traversal and SSRF-adjacent bugs when user input lands in a request URL — plus wider `log/slog` coverage on an existing rule and clearer taint-analysis messages for tracing where the untrusted value came from.

[gosec](#)

APPLICATION SECURITY

Web Application Security

Acunetix 360

Feedback



changelog · Oct 23, 2026

CHANGELOG

RANK

Acunetix 360 scans web applications and APIs to identify security vulnerabilities through automated testing.

Acunetix 360 added a default protocol field to website API responses and let custom roles send scan notifications to external recipients without full notification access.

WHAT SHIPPED · 2 FEATURES most completely described first ? what's the number?

01 Default protocol field in website API NEW 43

Website API responses now include a default protocol parameter, enabling retrieval of the default protocol configured for each website.

- Names the field but not the endpoint path or method. changelog-20261023-217daab0

02 External scan notifications for custom roles NEW 38

Custom roles can now send scan notifications to external recipients without being granted full access to all organizational notifications.

- Describes behavior but no config key or UI path given. changelog-20261023-217daab0

WAS THIS USEFUL? thumbs up thumbs down

GitGuardian Self-Hosted

Feedback



changelog · Oct 23, 2026

CHANGELOG ▸

GitGuardian Self-Hosted is an on-premises version of GitGuardian's platform that scans code repositories and CI/CD pipelines to detect leaked secrets and credentials.

Adds Wiz integration, per-source status filtering and views, unreachable-integration auto-recovery, `beat.metricsPort` Prometheus metrics, new public API endpoints (presence check, check-run skip), configurable ggshield API timeout, team perimeter settings, and audit log CSV secret-export detail.

NEW INTEGRATION Adds a Wiz integration that syncs active secret incidents from version control sources to Wiz daily as native secret findings, with detection context and a link back to GitGuardian (never the secret value); requires outbound HTTPS access to your Wiz tenant.

Adds source-status visibility — every source now shows `Monitored`, `Unmonitored`, `Unreachable`, `Archived`, or `Deleted` state — and lets you filter on that status from the perimeter page and incident list, and save it as a named view.

UPDATED INTEGRATION Adds automatic pause-and-resume for unreachable integrations (GitHub, GitLab, Bitbucket, Azure DevOps, Jira, Confluence, Slack, and Microsoft Teams on Self-Hosted): real-time ingestion and historical scans pause when a token expires or a provider is unreachable, and resume automatically once reconnected.

Adds `is all of` operator to the source-status filter.

Adds `beat.metricsPort` config key so the task scheduler exposes Prometheus metrics, and the chart creates a ServiceMonitor for it when ServiceMonitors are enabled.

+9 more

NEW DETECTION v2.172 new detectors

UPDATED DETECTION v2.172 improved detectors

NEW DETECTION v2.172 new checkers

NEW DETECTION v2.172 new analyzers

UPDATED DETECTION v2.172 analyzer update

NEW DETECTION v2.173 new detectors

UPDATED DETECTION v2.173 improved detectors

NEW DETECTION v2.173 new analyzer

UPDATED INTEGRATION AI Hooks expanded to Amazon Kiro and Junie CLI

↳ BREAKING ON UPGRADE

- ! Legacy analytics are removed in 2026.10: if in-app analytics are disabled on your instance, you must enable them before upgrading or your analytics dashboards will be lost.
- ! Background migrations must complete before an upgrade is accepted; attempting to upgrade while they run is refused with 'Not all required migrations have been applied' — wait for them to finish, then retry.
- ! Embedded cluster preflight checks now require at least 12 CPU cores and 48 GiB of memory (up from 8 cores and 30 GiB); a smaller VM fails the check on upgrade.

WAS THIS USEFUL?



GitGuardian Detection Engine

Feedback



changelog · Oct 23, 2026

CHANGELOG

RANK

GitGuardian Detection Engine scans source code repositories, commits, and pipelines to detect leaked secrets such as API keys, passwords, and credentials.

GitGuardian's Detection Engine (v2.174.0) adds ten new secret detectors, an SMTP validity checker, and a round of checker accuracy and reach improvements, while also retiring and consolidating several older detectors.

WHAT SHIPPED · 11 FEATURES most completely described first ? what's the number?

01 Detector removals and merges for cleanup

BREAKING

70

The `line_notify_token` detector has been removed. The `ftp_credentials_assignment` detector now only captures FTP secrets, not SFTP — SFTP secrets require the new `sftp_credentials_assignment` detector. The `azure_event_grid_access_key_with_host` detector has been merged into `azure_event_grid_access_key`, `grafana_service_account_token_with_host` into `grafana_service_account_token`, `kubernetes_jwt_with_host` into `kubernetes_jwt`, `planetscale_database_password_with_host_and_username` into `planetscale_database_password`, and `postgres_assignment_attached_port` / `postgres_assignment_no_port` into `postgres_assignment`.

— Every removed and merged detector named verbatim with its replacement.

changelog-20261023-7ab45329

02 Ten new secret detectors added

NEW

60

New detectors added for `sftp_credentials_assignment` SFTP credentials, Lago API keys, Composio project API keys, Composio organization API keys, Codex API keys, CARTO Basemaps API keys, Google Chat incoming webhook URLs, HubSpot CLI personal access keys, AmneziaWG VPN private keys, and Kubernetes bearer tokens stored in kubeconfig files.

— Names all ten detectors but no detection mechanism or config shown.

changelog-20261023-7ab45329

THINNER COVERAGE BELOW

03 Port-optional credential detection for FTP and MSSQL

IMPROVED

55

The `ftp_credentials_assignment` detector now handles secrets without a port, and the `mssql_assignment` detector now detects MSSQL credentials assigned without a

port.

– Both detectors named with the exact behavior change. [changelog-20261023-7ab45329](#)

04 Snowpark checker supports more account identifier formats

IMPROVED

55

The `snowpark_api_credentials` checker now supports short account identifiers, hostnames, and full Snowflake URLs.

– Names the three supported formats concretely. [changelog-20261023-7ab45329](#)

05 Custom host and proxy support across Azure, GitLab and LiteLLM checkers

IMPROVED

55

The Azure Entra Access Token checker and Azure Active Directory API Keys checker now accept a custom host, while the Azure Entra ID token checker, GitLab Deploy Token checker, and LiteLLM API key checker can now reach custom hosts through a proxy.

– Names five checkers and the exact capability each gained. [changelog-20261023-7ab45329](#)

06 Timeout added to AWS SES key checker

IMPROVED

50

The `aws_ses_keys` checker now has a timeout to reduce kills by the apikey-checker.

– Names the checker and the problem fixed, no numeric timeout given.

[changelog-20261023-7ab45329](#)

07 Snyk key checker supports new region

IMPROVED

50

The `snyk_key_v2` checker now supports the `SNYK-US-02` region.

– Exact checker and region named but scope is narrow. [changelog-20261023-7ab45329](#)

08 Azure Entra app secret detects national cloud hosts

IMPROVED

50

The `azure_entra_app_secret` detector now detects credentials declared against Microsoft national cloud sign-in hosts.

– Names detector and scope change, no host list given. [changelog-20261023-7ab45329](#)

09 Algolia monitoring checker validates higher-permission keys

IMPROVED

50

The `algolia_monitoring` checker now validates all Algolia keys with more permissions than the default search key.

– Clear scope change but no further mechanism detail. [changelog-20261023-7ab45329](#)

10 n8n checker accepts scheme-less hosts

IMPROVED

50

The `n8n` API key checker and `n8n` MCP access token checker now check keys and tokens found with a host written without its scheme.

– Specific checkers and input format named. `changelog-20261023-7ab45329`

11 SMTP credential validity checker NEW

30

Enables a validity checker for SMTP credentials.

– Single sentence, no mechanism or scope given. `changelog-20261023-7ab45329`

!--> BREAKING ON UPGRADE

- ! The `line_notify_token` detector has been removed.
- ! The `ftp_credentials_assignment` detector now only captures FTP secrets, not SFTP – SFTP secrets require the new `sftp_credentials_assignment` detector.
- ! The `azure_event_grid_access_key_with_host` detector has been merged into `azure_event_grid_access_key`.
- ! The `grafana_service_account_token_with_host` detector has been merged into `grafana_service_account_token`.
- ! The `kubernetes_jwt_with_host` detector has been merged into `kubernetes_jwt`.
- ! The `planetscale_database_password_with_host_and_username` detector has been merged into `planetscale_database_password`.
- ! The `postgres_assignment_attached_port` and `postgres_assignment_no_port` detectors have been merged into `postgres_assignment`.

WAS THIS USEFUL?



Bitnami Sealed Secrets

[Feedback](#)[v0.41.0](#)[NOTES ↗](#)[CODE ↗](#)[RANK](#)

A Kubernetes controller and tool for one-way encrypted Secrets

Sealed Secrets v0.41.0 makes the controller more resilient to live cluster changes: it now reloads sealing keys on the fly and self-heals Secrets that have been manually edited, both without requiring a pod restart.

↳ [WHAT SHIPPED](#) • [2 FEATURES](#) most completely described first [? what's the number?](#)

01 Self-healing of manually modified Secrets

[IMPROVED](#)

75

The controller now heals manually modified Secrets by restoring them to the state defined by their parent SealedSecret, without a pod restart. The `--skip-recreate` controller flag now also suppresses this restoration, whereas previously it only skipped recreation of deleted Secrets.

– Names exact flag and its changed scope, no usage example given [v0.41.0](#)

THINNER COVERAGE BELOW

02 Dynamic sealing key reload

[IMPROVED](#)

55

The controller dynamically detects new, updated, and deleted sealing key secrets at runtime, so keys can be added, relabeled, or removed without requiring a pod restart.

– Explains behavior change but no flag or config to act on [v0.41.0](#)

WAS THIS USEFUL?



gosec

Feedback



v2.30.0

NOTES ↗

RANK

Go security checker

gosec v2.30.0 adds a new rule to catch unescaped URL path elements, extends log/slog coverage for an existing rule, and improves taint-analysis messages.

↳ WHAT SHIPPED • 3 FEATURES most completely described first ? what's the number?

01 G125 rule for unescaped url.JoinPath elements NEW

70

A new **G125** rule detects unescaped elements passed to `url.JoinPath`, flagging potential XSS/injection risks in URL construction. It can be targeted directly, e.g. `gosec -include=G125 ./...`

Scan a module specifically for the new unescaped `url.JoinPath` rule to catch XSS/injection risks in URL construction.

```
$ gosec -include=G125 ./...
```

– Named rule ID and runnable scan command, but no mechanism detail beyond that. v2.30.0

THINNER COVERAGE BELOW

02 G706 extended to more log/slog methods IMPROVED

30

The **G706** rule now covers additional `log/slog` methods, broadening its existing checks.

– Names the rule and package but no list of methods or usage. v2.30.0

03 Sink naming in taint finding messages IMPROVED

25

Taint-analysis finding messages now name the sink involved, producing clearer output when a tainted value reaches a dangerous function.

– Describes the change but gives no example or exact message format. v2.30.0

WAS THIS USEFUL?



Levo

Feedback



October 20, 2026

NOTES

RANK

Levo continuous API Security Assurance  observe, detect, and protect your APIs.

Levo's October 2026 release makes authentication a first-class, endpoint-level signal across the inventory, Application Insights, and findings UI, while also letting users export web application scans as shareable files.

←→ WHAT SHIPPED · 6 FEATURES most completely described first ? what's the number?

01 Per-endpoint authentication visibility in inventory NEW

45

Every API endpoint now shows how it authenticates directly in the inventory view, surfacing auth method as a visible attribute per endpoint rather than requiring a separate lookup.

– Describes what changed but not the auth types or mechanism. October 20, 2026

02 CSV export auth columns replaced BREAKING

45

Authentication columns in two CSV exports have been replaced — existing automation or tooling that parses those columns will break on upgrade.

– States impact clearly but not the new column names. October 20, 2026

03 Weak authentication trends in Application Insights NEW

40

Application Insights gains a dedicated view for tracking weak authentication trends over time.

– Names the view but not what counts as weak or how trends are shown. October 20, 2026

04 Sensor tags in API inventory IMPROVED

30

Sensor tags are now propagated to the API inventory.

– Bare statement without detail on tag usage or scope. October 20, 2026

05 Exportable web application scans NEW

25

Web application scans can be saved and shared as a file.

– No file format or export mechanism specified. October 20, 2026

06 Easier discovery of custom-test findings IMPROVED

25

Custom-test findings are now easier to locate within the findings UI.

– Vague UI improvement with no specifics on mechanism.

October 20, 2026

↳ BREAKING ON UPGRADE

! Authentication columns in two CSV exports have been replaced — existing automation or tooling that parses those columns will break on upgrade.

WAS THIS USEFUL?



NETWORK SECURITY

◆ Firewalls & Network Defense

Sophos Firewall

Feedback



changelog · Oct 23, 2026

CHANGELOG ↗

RANK

Sophos Firewall is a next-generation network security appliance and software that protects networks through firewalling, intrusion prevention, VPN, web filtering, and threat detection.

Sophos Firewall v22.0 adds a CLI toggle to relax strict IPsec SA policy checks for third-party VPN peers that share Security Associations across multiple subnet pairs.

↳ WHAT SHIPPED · 1 FEATURE most completely described first ? what's the number?

01 CLI option to disable strict IPsec SA checks NEW 58

A new CLI command turns off strict policy checks for site-to-site IPsec VPN tunnels when third-party peers share Security Associations (SAs) across multiple subnet pairs, preventing incoming IPsec traffic from being dropped.

– Describes behavior and trigger but not exact command name

changelog-20261023-80580f1e

WAS THIS USEFUL?



Sophos DNS Protection

[Feedback](#)[changelog · Oct 23, 2026](#)[CHANGELOG](#)[RANK](#)

Sophos DNS Protection is a cloud-based service that filters DNS requests to block access to malicious, phishing, and unwanted websites across a network.

Sophos DNS Protection simplified onboarding from Sophos Firewall by collapsing manual Fusion location setup and DoH configuration into a single toggle.

←→ **WHAT SHIPPED · 1 FEATURE** most completely described first [? what's the number?](#)

01 One-step DNS Protection enablement from SFOS **IMPROVED**

63

In SFOS 23.0, enabling DNS Protection with a single setting now automatically handles Sophos Firewall onboarding and DoH configuration, replacing the previous manual process of creating a Sophos Fusion location and configuring firewall IPs. DNS filtering policies are then managed from Sophos Fusion.

Replace manual Sophos Fusion location creation and firewall IP config by turning on DNS Protection in a single step via SFOS 23.0.

 In Sophos Firewall (SFOS 23.0), go to the DNS Protection settings and turn on the **DNS Protection** toggle. Firewall onboarding and DoH configuration are applied automatically — no manual Sophos Fusion location or IP setup required.

– Names SFOS 23.0 and the toggle but omits deeper mechanism [changelog-20261023-6000cc6e](#)

WAS THIS USEFUL?



CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

Plexicus

[Feedback](#)[changelog · Oct 23, 2026](#)[CHANGELOG ↗](#)

Plexicus validates security findings with evidence and helps your team fix what matters. AI Swarm Pentest, Deep Code Analysis, Remediation and XBOM.

PlexiFlow automation editor rebuilt with undo, visual conditions, searchable pickers, and a schedule builder.

Adds undo support to the PlexiFlow automation editor.

Adds visual conditions to the PlexiFlow automation editor.

Adds searchable pickers to the PlexiFlow automation editor.

Adds a schedule builder to the PlexiFlow automation editor.

[NEW SUPPORTED PLATFORM](#)[C#/.NET and Razor AI-SAST support](#)

WAS THIS USEFUL?



DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

XFA

[Feedback](#)[changelog · Oct 23, 2026](#)[CHANGELOG ↗](#)

XFA Desktop Application adds NixOS support, installable without root into a nix profile, with auto-update and optional admin-managed system configuration.

[NEW SUPPORTED PLATFORM](#)[NixOS support for XFA Desktop Application](#)

WAS THIS USEFUL?



Tenzir

Feedback ⓘ changelog · Oct 23, 2026 CHANGELOG ↗ RANK

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

Tenzir added non-interactive machine credentials for organizations on the Platform and improved Helm chart handling for slow node startups.

⌵--> WHAT SHIPPED · 1 FEATURE most completely described first ? what's the number?

01 Slow node startup support in Helm charts IMPROVED 30

Tenzir Helm Charts (v0.2.0) now support slow node startups.

- Bare statement of support, no detail on mechanism changelog-20261023-492a9fb7

WAS THIS USEFUL?  

IDENTITY, ACCESS & DATA PROTECTION

Veeam Kasten

[Feedback](#)[changelog · Oct 23, 2026](#)[CHANGELOG >](#)**RANK**

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

Kasten K10 9.0.9 adds restartless per-service log-level control, per-policy timeout annotations, and new Helm-configured concurrency limiters, alongside Kubernetes 1.36 support and expanded [SBOM/VEX](#) publishing, plus several breaking changes around [CPU](#) architecture, [RBAC](#) permissions, and ActionPodSpec validation.

← **WHAT SHIPPED · 11 FEATURES** most completely described first [? what's the number?](#)

01 Restartless log-level control

NEW

91

The `logLevel0overrides` Helm value (requires `features.restartlessLogLevelChange`, enabled by default on new installs) lets operators set the log level (`info` , `debug`) of individual Veeam Kasten services without restarting them, and the global Kasten log level can also be changed without a restart. New operation pods inherit the current log level of the service that creates them, with explicit `LOG_LEVEL` settings and command-line logging options taking precedence. With the feature enabled, Kanister now follows the same log levels as other services, so a `logLevel` other than `info` or `debug` falls back to `info` ; the setting is the default for fresh installs but is not applied automatically on upgrades using `--reuse-values` and must be added explicitly.

Enable per-service log-level overrides so you can debug the catalog service at `debug` verbosity without restarting it or affecting other services.

```
$ helm upgrade k10 kasten/k10 --reuse-values \
  --set features.restartlessLogLevelChange=true \
  --set logLevel0overrides.catalog=debug
```

— Flag, default behavior, precedence rules, and a runnable command.

[changelog-20261023-d4cba05c](#)

02 Per-policy action timeout annotations

NEW

79

Policy objects can now set action-phase timeout overrides via the annotations `k10.kasten.io/backup-timeout` , `k10.kasten.io/restore-timeout` , `k10.kasten.io/retire-timeout` , and `k10.kasten.io/blueprint-resource-`

`hooks-timeout` , letting operators tune timeouts per policy instead of relying on global defaults.

Tune per-policy backup, restore, and retire timeouts independently without touching global defaults — useful for policies protecting large or slow-to-snapshot workloads.

```
$ kubectl annotate policy my-backup-policy \
  k10.kasten.io/backup-timeout=2h \
  k10.kasten.io/restore-timeout=3h \
  k10.kasten.io/retire-timeout=30m
```

– Four annotations named plus a runnable kubectl example.

changelog-20261023-d4cba05c

03 Concurrency limiters for repository and VM snapshot operations

NEW

72

A new `limiter.repositoryOperationsPerCluster` Helm value (default: 3) caps the number of concurrent background repository maintenance runs and storage usage scans. Separately, Kasten now releases the `limiter.vmSnapshotsPerCluster` token immediately after storage cuts snapshots of all VM volumes rather than waiting for the full backup to finish, letting VM backups complete faster.

Limit concurrent background repository maintenance and storage scans to 2 to reduce pressure on object storage during peak backup windows.

```
$ helm upgrade k10 kasten/k10 --reuse-values \
  --set limiter.repositoryOperationsPerCluster=2
```

– Named Helm values with defaults; one has a runnable command.

changelog-20261023-d4cba05c

04 ActionPodSpec schema validation on create/update

BREAKING

71

`ActionPodSpec` objects are now validated against a schema on create and update: unknown fields under `spec` are rejected, and resource quantities must be an integer or a quoted string (e.g., `cpu: '0.5'` or `cpu: 500m`) rather than a bare decimal like `cpu: 0.5`. Existing objects with bare decimals continue working until their next update.

– Concrete validation rule with example values and migration note.

changelog-20261023-d4cba05c

05 ActionPodSpecBinding scoping change, install-namespace use deprecated

DEPRECATED

70

`ActionPodSpecBinding` set in the protected application's namespace is now applied to `repository-server` datamover pods (`data-mover-svc-*`) and `delete-collection` pods, overriding any binding set in the install namespace for single-namespace policy runs. Using `ActionPodSpecBinding` in the Veeam Kasten install namespace to configure the `repository-server` or `delete-collection` pod is now deprecated and will be removed in a future release.

– Clear before/after behavior and a deprecation path. [changelog-20261023-d4cba05c](#)

THINNER COVERAGE BELOW

06 OpenVEX and SBOM publishing improvements

NEW

57

Each release now publishes an OpenVEX document that third-party SBOM scanners can process to suppress vulnerability findings for Go modules whose vulnerable code is absent from Veeam Kasten binaries. Published SBOMs now identify each image's root package by image name, Kasten version, image digest, and package URLs (`pkg:oci` , `pkg:generic`) to support vulnerability scanner VEX matching.

– Named formats and identifiers but no direct action step. [changelog-20261023-d4cba05c](#)

07 RBAC permission requirement for csinodes

BREAKING

48

Deployments using `rbac.create=false` must now grant `list` permission on `csinodes` in the `storage.k8s.io` API group to the Veeam Kasten service account, or operations that provision PVCs will fail.

– Specific, actionable RBAC fix with minimal added context. [changelog-20261023-d4cba05c](#)

08 Kubernetes 1.36 support added, 1.32 dropped

BREAKING

40

Veeam Kasten 9.0.9 adds support for Kubernetes 1.36 while dropping support for Kubernetes 1.32.

– Bare version support change with no migration detail. [changelog-20261023-d4cba05c](#)

09 imageStreamImageResolveSec timeout validation

BREAKING

40

The Helm value `timeout.imageStreamImageResolveSec` must now be left empty or set to at least a documented minimum; installs and upgrades that set a value below that minimum or a negative value now fail Helm chart validation.

– Named config key but exact minimum value not given. [changelog-20261023-d4cba05c](#)

On x86-64 clusters, Veeam Kasten now requires an x86-64-v3 CPU (Intel Haswell / AMD Excavator) or newer; clusters running on older x86-64 processors are no longer supported.

– States requirement but offers no verification steps. `changelog-20261023-d4cba05c`

11 Temporary image pull secret copies for blueprint actions

NEW

Veeam Kasten can now create automatic, temporary copies of its image pull secrets in application namespaces when executing blueprint actions.

– Thin one-line description with no config surface named. `changelog-20261023-d4cba05c`

---> BREAKING ON UPGRADE

- ! `timeout.imageStreamImageResolveSec` must be empty or at least the documented minimum; installs and upgrades that set a value below the minimum or a negative value fail Helm chart validation.
- ! On x86-64 clusters, Veeam Kasten now requires x86-64-v3 CPU (Intel Haswell / AMD Excavator) or newer; clusters running on older x86-64 processors will not be supported.
- ! Kubernetes 1.32 is no longer supported.
- ! Deployments using `rbac.create=false` must grant `list` permission on `csinodes` in the `storage.k8s.io` API group to the appropriate service account, or operations that provision PVCs will fail.
- ! `ActionPodSpec` objects with unknown fields under `spec` or bare decimal resource quantities (e.g., `cpu: 0.5`) are now rejected on create/update; existing objects with bare decimals continue working until next update.
- ! With `features.restartlessLogLevelChange` enabled, Kanister now follows the same log levels as other Veeam Kasten services: a `logLevel` other than `info` or `debug` falls back to `info`, so a setting of `error` will cause Kanister to log more after the upgrade.
- ! Enabling log-level changes without a restart (`features.restartlessLogLevelChange=true`) is the new default for fresh installs but is NOT set automatically on upgrades using `--reuse-values`; the setting must be added explicitly.

WAS THIS USEFUL?



NVIDIA SkillSpector

[Feedback](#)[v2.13.1](#)[NOTES >](#)

Security scanner for AI agent skills. Detect vulnerabilities, malicious patterns, security risks, prompt injection, data exfiltration, and supply-chain risks in Claude Code, Codex, and MCP skills before you install them.

v2.13.1 enforces atomic, no-follow report and baseline writes; rejects invalid flag combinations for `--recursive` and `--mcp-registry` with exit code 2; and surfaces batch gap-fill failures via `gap_fill_status: "incomplete"`.

↳ GET THIS VERSION

```
$ git clone --branch v2.13.1
https://github.com/NVIDIA/SkillSpector.git
# already have the repo? check out this version:
$ git checkout v2.13.1
```

Writes report files (`scan` , `scan --recursive` , `scan --mcp-registry` , and `--output`) and baselines atomically through an already-opened, no-follow parent directory; `skillspector baseline <path> -o -` writes the baseline as JSON to stdout.

Rejects `--use-shipped-baseline` with exit code 2 when `scan --recursive` detects one or more child skills, before any report is written.

Rejects `scan --mcp-registry` combined with `--use-shipped-baseline` , `--transitive` , `--transitive-depth` , `--transitive-allow-prefix` , or `--transitive-deny-prefix` with exit code 2 before the registry is read or a report is written.

Reports failed batch gap-fill passes as incomplete with `gap_fill_status: "incomplete"` , failure reasons, and at least a CAUTION recommendation; the batch run exits with code 2.

Reports a complete recursive scan whose highest score is MEDIUM (21-50) as CAUTION instead of SAFE, matching child reports.

UPDATED DETECTION [P2 hidden-instruction detection scope correction](#)

NEW DETECTION [HIGH MP3 finding for state/memory adoption instructions](#)

UPDATED DETECTION [TM1 repeated Python assignment handling](#)

↳ BREAKING ON UPGRADE

- ! `scan --recursive` now rejects `--use-shipped-baseline` with exit code 2 when child skills are detected; previously the option was silently ignored.
- ! `scan --mcp-registry` now rejects `--use-shipped-baseline`, `--transitive`, `--transitive-depth`, `--transitive-allow-prefix`, and `--transitive-deny-prefix` with exit code 2; previously these options were silently ignored.
- ! A complete recursive scan with a highest score of MEDIUM (21-50) now exits with CAUTION instead of SAFE.

WAS THIS USEFUL?



// END OF TRANSMISSION ■

The Cyber Toolchain · curated daily · October 23, 2026

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

▷ **Subscribe**

Feedback on this issue