THE CYBER TOOLCHAIN

NO. 055

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 24, 2026 · EVERY DAY

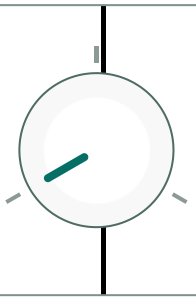
The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // **CONTENTS** SHOW 21 tools

OFFENSIVE SECURITY

vim ? help

◆ AI-Powered Offensive Security

T3MP3ST

Feedback ⓘ changes since 2026-08-12 CODE ↗

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

T3MP3ST adds Novita AI as a native LLM provider and enables Claude Code session resume across kill-chain phases.

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-08-12 https://github.com/elder-plinius/T3MP3ST.git
# already have the repo? check out this version:
$ git checkout commits-2026-08-12
```

Adds `NOVITA_API_KEY` environment variable to enable Novita AI as a first-class LLM provider, dispatched through the OpenAI-compatible endpoint at `https://api.novita.ai/openai/v1` with a default model and curated model catalog entries.

Adds `T3MP3ST_TRUST_CLAUDE_SESSION` environment variable (set to `1`) to enable Claude Code session resume across kill-chain phases, persisting session state between agent turns instead of starting fresh each time.

Adds optional resetSession() method to the `LLMProviderAdapter` interface, allowing providers that support resumed backend sessions to expose a clean-session escape hatch.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Web Application Security

Invicti

Feedback ⓘ 1 RELEASE · 2026-08-24 CHANGELOG ↗

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

> Invicti adds application- and collection-level scan scheduling, ephemeral API targets for CI/CD environments, and incremental scanning support in scan-cli, alongside several smaller improvements to SSO, integrations, and API discovery.

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

01 **Incremental scanning via scan-cli environment variable** NEW

75

Adds the `INVICTI_INCREMENTAL_SCAN` environment variable to `scan-cli`, limiting a scan to new or changed endpoints to reduce scan time in CI/CD pipelines.

— Names exact env var and mechanism, but no usage example shown.

changelog-20260824-d73297dd

02 **Exclude API action in API Discovery** IMPROVED

70

Adds an Exclude API action in API Discovery, replacing Hide API, which labels APIs as third-party and requires a reason for exclusion. In the API Discovery view, users open the API's action menu, select Exclude API, choose Third-party as the type, and enter a reason.

Exclude a detected third-party API from discovery results so it no longer appears in the API Catalog.

📍 In API Discovery, locate the API, open its action menu, select Exclude API, choose Third-party as the type, and enter a reason for the exclusion.

— Includes exact UI steps to perform the action via usage example.

changelog-20260824-d73297dd

THINNER COVERAGE BELOW

03 **Scheduled scans for entire applications and collections**

IMPROVED

55

Adds scheduled scans for entire applications or collections, automatically running DAST scans across all included targets on a chosen recurrence; previously schedules were per-target only.

– Clear before/after but no exact config or endpoint given. changelog-20260824-d73297dd

04 **Ephemeral API targets with dynamic base URL** NEW

55

Adds ephemeral API targets with a dynamic base URL that resolves at scan time, enabling scanning of temporary or CI/CD-provisioned environments without manual target reconfiguration.

– Explains mechanism and use case but no concrete configuration steps.

changelog-20260824-d73297dd

05 **Exponential backoff with jitter on rate-limited scans**

IMPROVED

55

Scan engine now applies exponential backoff with jitter when retrying requests that receive a 429 Too Many Requests response with no `Retry-After` header, improving crawl coverage on rate-limited targets.

– Describes mechanism and trigger condition but is automatic, non-actionable by users.

changelog-20260824-d73297dd

06 **Downloadable large payloads in vulnerability details** IMPROVED

55

Request and response payloads over 2 MB in vulnerability details are now offered as a download instead of being rendered inline, supporting very large scan results.

– Names exact size threshold and behavior change. changelog-20260824-d73297dd

07 **Integration field mapping enhancements for Jira, Azure Boards, GitHub, GitLab**

NEW

50

Adds `{Asset URL}` placeholder support in Jira, Azure Boards, GitHub, and GitLab integration field mappings, and adds custom Jira fields of type Label to integration field mapping, enabling automatic tagging of Jira issues created by Invicti.

– Names placeholder and field type but no full mapping workflow shown.

changelog-20260824-d73297dd

08 **Permission-based filtering in API Catalog** IMPROVED

50

API Catalog now filters displayed targets based on the user's collection-level permissions, removing the requirement to have account-wide target access.

— States before/after behavior but no exact UI path or setting.

changelog-20260824-d73297dd

09 **SSO settings enhancements** NEW 45

Adds a unique organization identifier on the SSO settings page that can be copied for use when registering Invicti as a SAML service provider, and adds SSO login support for organizations whose identity provider certificate is stored in bare base-64 DER format.

— Names the UI location and certificate format but lacks setup detail.

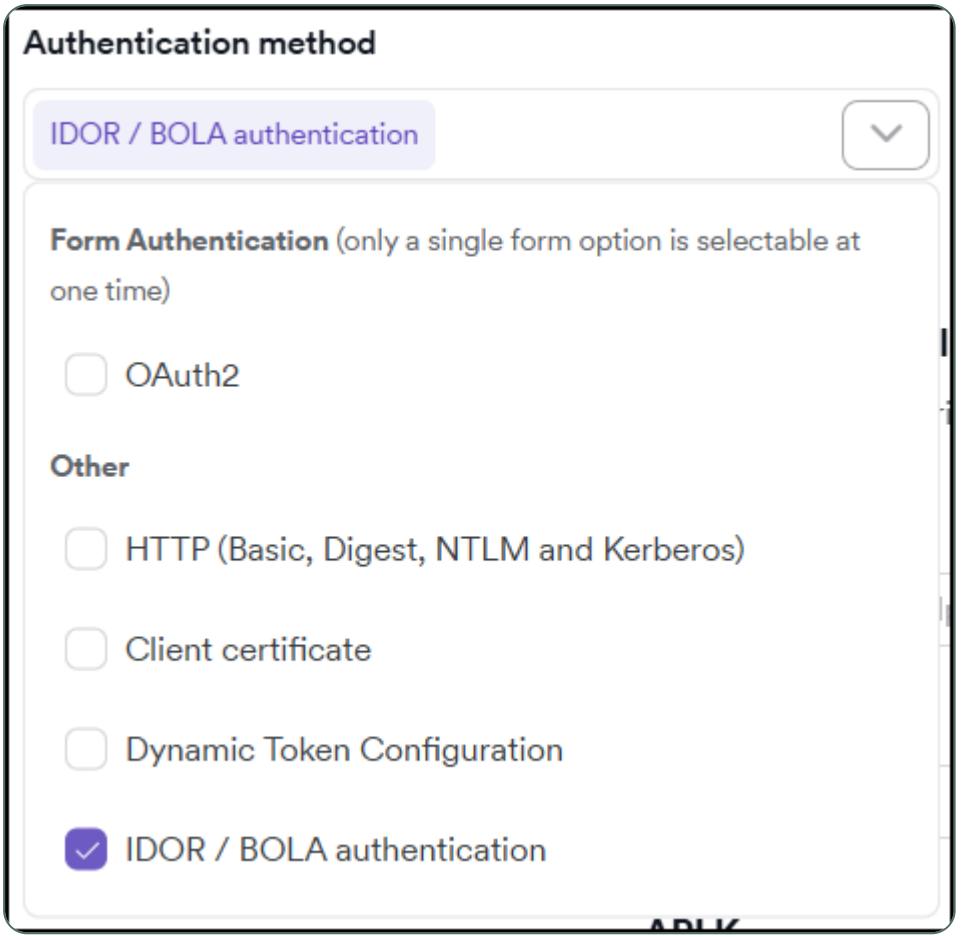
changelog-20260824-d73297dd

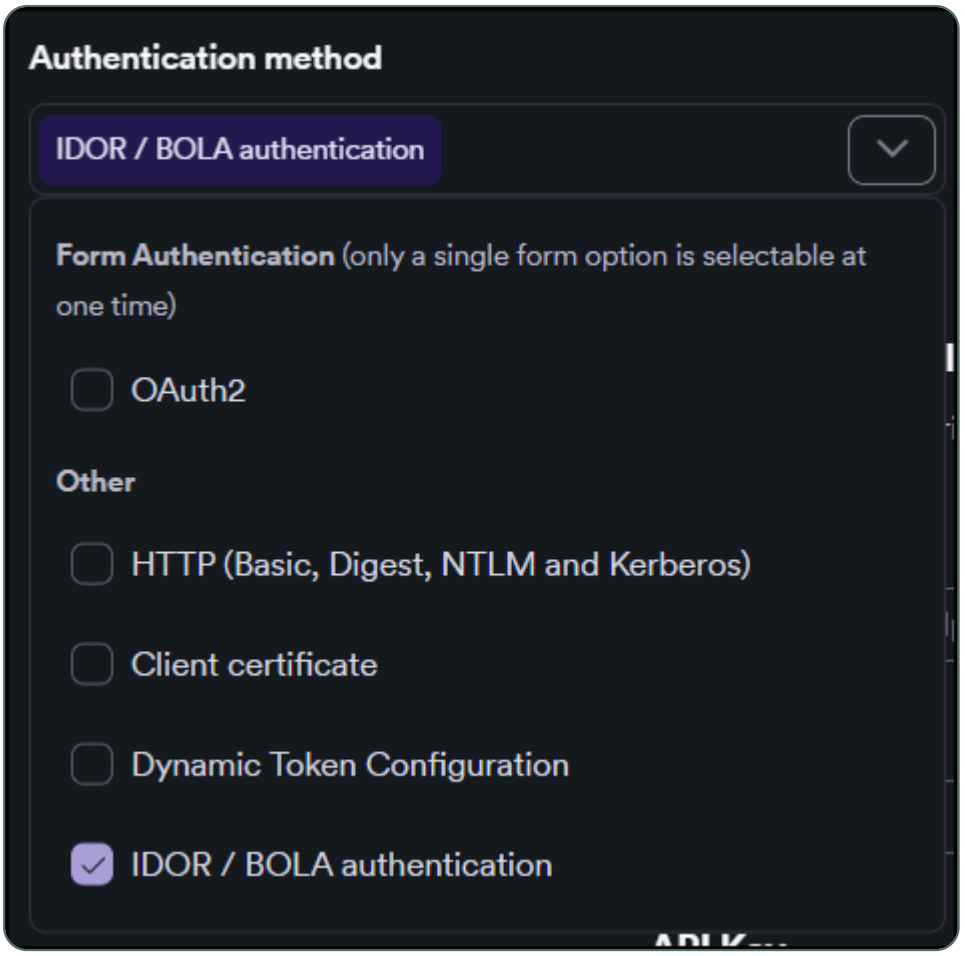
10 **scan-cli runtime updated to .NET 10** IMPROVED 30

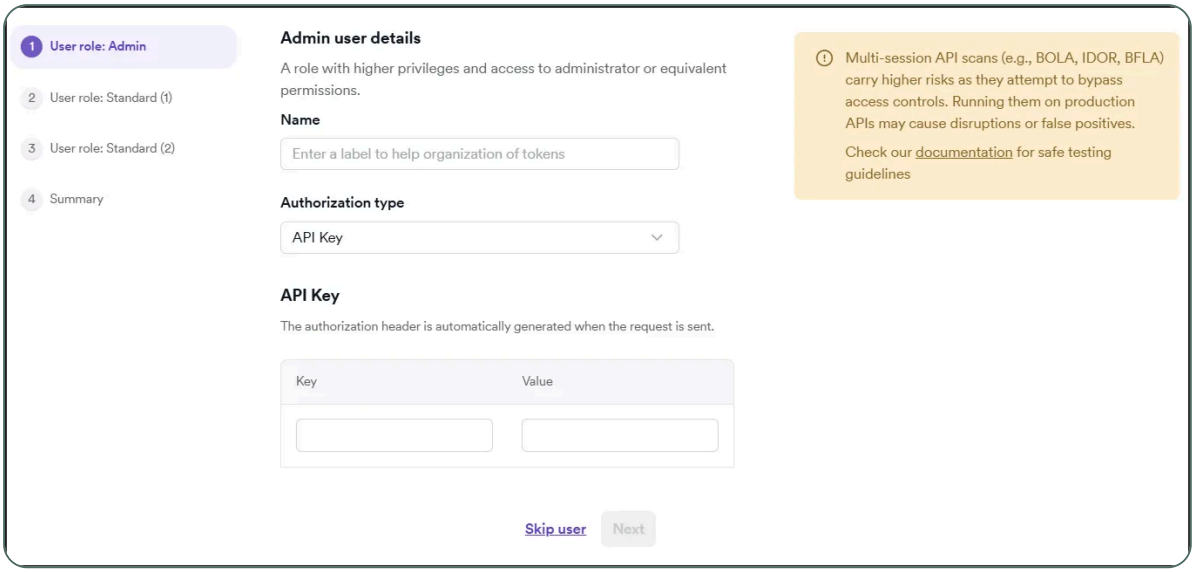
Updates the `scan-cli` runtime to .NET 10.

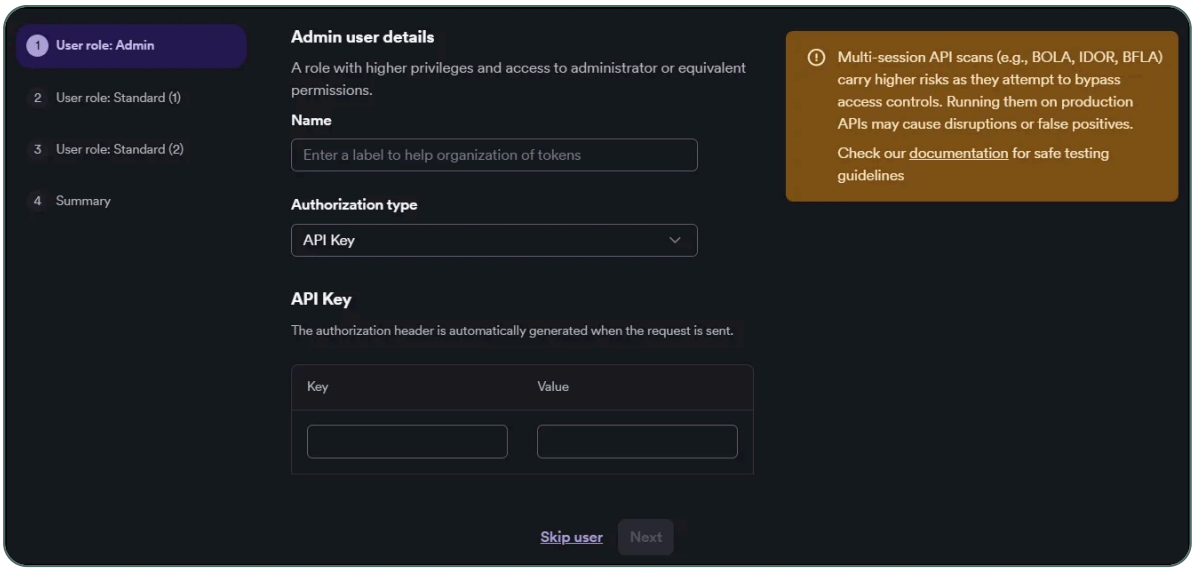
— Bare version bump with no further detail. changelog-20260824-d73297dd

└──▷ **ALSO FROM THESE RELEASES**




Authentication method
IDOR / BOLA authentication
Form Authentication (only a single form option is selectable at one time)
OAuth2
Other
HTTP (Basic, Digest, NTLM and Kerberos)
Client certificate
Dynamic Token Configuration
IDOR / BOLA authentication


1 User role: Admin
2 User role: Standard (1)
3 User role: Standard (2)
4 Summary
Admin user details
A role with higher privileges and access to administrator or equivalent permissions.
Name
Enter a label to help organization of tokens
Authorization type
API Key
API Key
The authorization header is automatically generated when the request is sent.
Key
Value
Skip user
Next
Multi-session API scans (e.g., BOLA, IDOR, BFLA) carry higher risks as they attempt to bypass access controls. Running them on production APIs may cause disruptions or false positives.
Check our documentation for safe testing guidelines



WAS THIS USEFUL?

PortSwigger Burp Suite

Feedback ⓘ 1 RELEASE · 2026-08-24

BLOG ↗

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

> Burp Suite 2026.8 focuses on workflow and reporting refinements: customisable title bar actions, richer manual issue documentation, and clearer evidence highlighting for AT-raised issues.

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

01 **Customisable title bar actions** NEW 33

Practitioners can pin frequently used functions directly to the title bar for faster access, rather than navigating menus each time.

— Describes benefit but no exact UI path or config

Professional / Community 2026.8 (2026-0…

02 **Multiple evidence items in manual issues** IMPROVED 33

When manually creating issues, users can now attach multiple evidence items to a single issue entry, allowing richer documentation of findings.

— Explains capability but no mechanism or limit given

Professional / Community 2026.8 (2026-0…

03 **Evidence highlighting for Burp AT issues** IMPROVED 31

Issues raised by Burp AT now include evidence highlighting, making it easier to identify the relevant portions of captured traffic.

— States benefit but no detail on highlighting mechanism

Professional / Community 2026.8 (2026-0…

WAS THIS USEFUL? 👍 👎

DataDome

Feedback ⓘ 1 RELEASE · 2026-08-24 BLOG ↗

DataDome is a bot management and API protection platform that defends against automated attacks, web scraping, and credential abuse.

> DataDome extended two integrations this window: the CloudFront Lambda@Edge integration gained a newer Node runtime, and the Tyk module added GraphQL detection, host override support and redirect handling.

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

01 **Tyk module GraphQL and host detection** NEW 86

The Tyk module (1.4.0) adds a `datadome_graphql_endpoint` config option to define one or more comma-separated paths used to detect GraphQL requests, defaulting to `graphql` (e.g. `datadome_graphql_endpoint = graphql,api/graphql,query`). It also adds `datadome_use_x_forwarded_host` to support host override via the `X-Forwarded-Host` header (`datadome_use_x_forwarded_host = true`), and adds support for 301/302 redirects.

Route GraphQL traffic detection across multiple non-standard endpoints in a Tyk plugin config.

```ini
datadome_graphql_endpoint = graphql,api/graphql,query
```

Enable host override via the X-Forwarded-Host header when DataDome sits behind a reverse proxy that rewrites the Host.

```ini
datadome_use_x_forwarded_host = true
```

— Names exact config keys, defaults and example values Tyk module 1.4.0 (2026-08-24)

THINNER COVERAGE BELOW

02 **nodejs26.x runtime for CloudFront integration** IMPROVED 35

The DataDome CloudFront Lambda@Edge integration now supports the `nodejs26.x` Lambda runtime.

— Names the runtime but no setup detail product docs

WAS THIS USEFUL?  

◆ SAST / SCA / Code Security

Snyk

Feedback ⓘ 1 RELEASE · 2026-08-24 DOCS ↗ BLOG ↗

The official changelog for the Snyk AI Trust Platform. Discover what's new in our security intelligence, AI-powered tools, and latest product enhancements.

> Snyk shipped a redesigned UI centered on faster navigation, including command-palette search, Dark Mode, a new breadcrumb-based scope switcher, and a consolidated Settings hub.

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

01 **Command-palette navigation search** NEW 75

A `Cmd/Ctrl+K` shortcut opens a search box that jumps directly to any page or setting without menu-hunting, useful now that the sidebar is condensed to core areas.

Jump directly to any Snyk page or setting without navigating the sidebar — useful after the sidebar is condensed to core areas only.

> 📍 In the Snyk UI, press Cmd+K (macOS) or Ctrl+K (Windows/Linux), then type the name of the setting or page you want (e.g. Integrations or Policies) and select the result.

— Exact shortcut and steps given, mechanism clear 2026-08-24-434df230

02 **Breadcrumb bar for scope switching** NEW 62

Replaces the classic multi-scope sidebar with a single breadcrumb bar supporting one-click scope switching via per-level drop-downs for Tenant, Group, and Organization.

— Describes before/after and named scope levels, no exact steps 2026-08-24-434df230

03 **Dark Mode theming** NEW 60

Adds Dark Mode with System/Light/Dark options, selectable from the user account menu and consistent across all pages.

Enable Dark Mode for a consistent dark-themed experience across Snyk and other dark-mode-enabled cyber tools.

> 📍 In the Snyk UI, open the user account menu (top-right), navigate to appearance preferences, and select Dark (or System) from the Dark Mode options.

— Named options and UI path but no deeper mechanism 2026-08-24-434df230

THINNER COVERAGE BELOW

04 **Consolidated Settings hub** NEW 54

Consolidates all settings-related pages into a single context-aware Settings hub, with the left sidebar condensed to core areas: Analytics, Inventory, Projects, Issues, Policies, and Settings.

— Names the consolidated sidebar areas but no interaction detail 2026-08-24-434df230

05 **Toggle between classic and new navigation** NEW 28

Users can switch freely between the classic and new navigation via the user account menu.

— Single-line mention with minimal mechanism 2026-08-24-434df230

WAS THIS USEFUL? 👍 👎

OWASP dependency-track

Feedback ⓘ 1 RELEASE · 2026-08-24

NOTES ↗

Dependency-Track is an intelligent Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain.

> Dependency-Track 5.0.5 improves OSV vulnerability data ingestion by speeding up full archive downloads.

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

01 **Faster OSV full archive downloads** IMPROVED 35

Dependency-Track now leverages OSV's `modified_id.csv` list to optimize full vulnerability archive downloads, reducing unnecessary data transfer.

— Names the mechanism file but no numbers or config exposed. 5.0.5

WAS THIS USEFUL? 👍 👎

StepSecurity

Feedback

ⓘ

2 RELEASES · 2026-08-20 → 2026-08-24

BLOG ↗

StepSecurity is a security platform that hardens CI/CD pipelines by reducing attack surface and detecting suspicious activity in GitHub Actions workflows.

> StepSecurity added AWS as a second OIDC federation provider for minting scoped API tokens, and shipped ARC Harden Runner v2.19.0 with configurable image pull policy and cluster-wide deny list egress enforcement.

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

01

AWS OIDC federation for API token minting NEW

93

Adds AWS as a second OIDC federation provider for StepSecurity trust policies alongside GitHub Actions — EKS, EC2, Lambda, and any workload that can call AWS STS can mint scoped StepSecurity API tokens without a long-lived key. AWS trust policies match on the issuer URL of the account's outbound federation, the 12-digit AWS account ID, and an optional role ARN (leave blank to trust any role in the account, or specify one to pin to a single workload), and carry the same max session duration and permissions allowlist controls already available to GitHub Actions policies. The provider is configured at organization scope via the StepSecurity API (Org Access) trust policy form, which now opens with a provider selector (GitHub Actions or AWS) showing the matching identity fields.

Configure an org-scope trust policy in StepSecurity that allows any IAM role in a specific AWS account to mint API tokens — useful for giving an EKS cluster-wide workload identity access without storing a key.

> 📍 In the StepSecurity console, go to Organization › Trust Policies › New Policy, set Provider to AWS , enter your 12-digit AWS account ID, leave Role ARN blank to trust any role in the account, set a max session duration, and add the required permissions to the allowlist.

Pin a trust policy to a single Lambda function's execution role so only that workload can mint a StepSecurity API token.

> 📍 In the StepSecurity console, go to Organization › Trust Policies › New Policy, set Provider to AWS , enter the 12-digit AWS account ID, and enter the full role ARN (e.g. arn:aws:iam::123456789012:role/my-lambda-role) to restrict minting to that single workload.

— Exact matching fields and UI steps for both trust-all and pinned policies.

Mint StepSecurity API Tokens from AWS W…

02

Configurable image pull policy for ARC Harden Runner NEW

85

Adds `env.imagePullPolicy` and `tetragon.imagePullPolicy` Helm values to control image pull behavior for ARC Harden Runner and Tetragon images, enabling `IfNotPresent` for clusters that pre-pull images or operate behind constrained registries.

Stop ARC Harden Runner from pulling images on every pod start in air-gapped or registry-constrained clusters by setting pull policy to `IfNotPresent` in your Helm values file.

```yaml
env:
  imagePullPolicy: IfNotPresent
tetragon:
  imagePullPolicy: IfNotPresent
```

— Names exact Helm keys and gives runnable config snippet.

ARC Harden Runner v2.19.0 (2026-08-24)

---

03 **Deny list egress enforcement extended to ARC Harden Runner**

IMPROVED

60

Extends deny list egress policy enforcement to ARC Harden Runner — policies attached at Cluster scope in the Policy Store now block specific destinations across every job in that cluster without requiring workflow file changes.

— Describes scope and mechanism but no concrete example or command.

ARC Harden Runner v2.19.0 (2026-08-24)

WAS THIS USEFUL? 👍 👎

Mend.io Mend Platform

Feedback ⓘ 1 RELEASE · 2026-08-23

NOTES ↗

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend Platform's biggest addition this window is an AI Bill of Materials report for inventorying AI models, prompts, and agents, alongside account-level global workflows, Chainguard support in container hardened-image detection, several Renovate config additions, and a reorganized Administration sidebar.

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

01 **AI Bill of Materials (AI-BOM) report** NEW 78

New `AI-BOM` report available through the Mend Platform reporting interface and API, generating an inventory of detected AI entities — models, system prompts, agent configurations, tools, and agents — at organization, application, and project scopes. Exports use industry-standard `CycloneDX 1.7` and `SPDX 3.0.1` formats with metadata-only content to preserve data privacy; data is populated only for scans performed after the 24-August-2026 release date.

— Names formats and scope but no concrete API endpoint given. product docs

02 **Chainguard support in hardened image detection** NEW 62

Adds Chainguard as a supported source in hardened image detection, incorporating Chainguard-specific vulnerability data, VEX information, and detection of Chainguard image layers and base images. Surfaces Chainguard VEX status and branding directly within the risk factors columns across the Mend Container UI for Chainguard-based images and findings.

— Explains mechanism and UI surface but no exact command or setting. product docs

03 **Renovate config additions: overrideDescription and devcontainer folder patterns**

NEW 62

Adds `overrideDescription` option to the Renovate config, allowing custom descriptions to be set on dependencies. Adds folder pattern support to `managerFilePatterns` for the `devcontainer` manager, broadening which Dev Container files are detected.

— Names exact config keys but gives no syntax example. product docs

THINNER COVERAGE BELOW

04 **Account-level global workflows** NEW 55

Introduces Account-Level (Global) Workflows, letting administrators define workflows centrally and propagate them to selected organizations, with controls over whether org-level admins can enable or disable them locally. Adds comprehensive API support for managing global workflows.

— Describes mechanism but no endpoint names or config keys given.

Version 26.8.1 (23-August-2026)

05 **Administration sidebar and AI Usage tab reorganization**

IMPROVED 55

Updates the Administration page sidebar with a categorized, collapsible navigation structure aligning with Application and Project pages. Moves AI Usage settings from the General tab into a dedicated `AI Usage` tab under a new `AI` category, and adds sub-headers for `AI`, `Code`, and `Dependencies` within Engine Settings.

Adjust AI Usage settings after the tab reorganization in the Administration page.

> 📍 In the Administration page, open the sidebar, navigate to the `AI` category, and select the `AI Usage` tab to configure AI Usage settings.

— Exact navigation path given but no config keys or API surface.

Version 26.8.1 (23-August-2026)

06 **Renovate onboarding flow improvements** IMPROVED 30

The onboarding summary view now shows the `What to Expect` section first, improving the onboarding flow for new repositories. The onboarding UI also clarifies that security PRs do not count against PR limits.

— Thin UI-only descriptions with no configurable surface named. product docs

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Malware Analysis

YARA-X

Feedback ⓘ 1 RELEASE · 2026-08-24 NOTES ↗

A rewrite of YARA in Rust.

> YARA-X v1.20.0 adds an `--ignore-invalid-rules` CLI flag with a matching Python API option, introduces experimental `msi`, `vba`, and `olecf` file-format modules, and speeds up scanning with SIMD-accelerated matching and faster rule deserialization, alongside new per-pattern match limits in the C and Go APIs.

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

01 `--ignore-invalid-rules` flag for skipping bad rules NEW

85

Adds `--ignore-invalid-rules` CLI option to skip rules that fail to compile instead of aborting a scan, and exposes the same behavior in the Python API via `ignore_invalid_rules`.

Scan a directory with a ruleset that contains some invalid rules, skipping failures instead of aborting.

```
$ yr scan --ignore-invalid-rules rules/ /path/to/samples/
```

— Exact flag, Python param, and runnable command given v1.20.0

02 Per-pattern match limits in C and Go APIs NEW

75

Adds `yrx_scanner_max_matches_per_pattern` to the C API and `Scanner.MaxMatchedPerPattern` to the Go API to cap the number of matches recorded per pattern.

— Names exact symbols in both APIs but no usage example v1.20.0

THINNER COVERAGE BELOW

03 `rlib` crate types for capi and py NEW

55

Adds `rlib` crate types to `yara-x-capi` and `yara-x-py` to allow linking into wrapper crates.

— Names crates and purpose, no example given v1.20.0

04 Experimental MSI, VBA, and OLECF modules NEW

50

Implements experimental `msi`, `vba`, and `olecf` modules for parsing those file formats in YARA rules.

— Names three new modules but no usage detail v1.20.0

05 **lnk module ShellItems and malformed section parsing** IMPROVED 45

Extends the `lnk` module to parse ShellItems and malformed sections.

— Names module and parsed structures, no example v1.20.0

06 **Faster rule deserialization via automata serialization** IMPROVED 40

Serializes Aho-Corasick automata directly with compiled rules for faster deserialization.

— Explains mechanism but no numbers v1.20.0

07 **Improved atom extraction and scan constraints** IMPROVED 40

Improves atom extraction heuristics and applies file size/header constraints only to regular expressions for better scan performance.

— Describes change but no measurable impact v1.20.0

08 **SIMD-accelerated masked literal matching** IMPROVED 35

Implements SIMD-accelerated masked literal matching for faster pattern scanning.

— States mechanism but no benchmark or scope v1.20.0

09 **Language server enum-aware code completion** IMPROVED 30

Improves code completion in the language server by distinguishing enums from other fields.

— Names behavior change but no config or command v1.20.0

10 **Playground UI theme support** NEW 30

Adds light/dark theme support to the playground UI.

— Simple UI addition, no further detail v1.20.0

11 **Python API type annotations** IMPROVED 25

Adds type annotations to match and return data in the Python API.

— Bare mention, no specifics on scope v1.20.0

12 **Warning for unintentional patterns in a set** IMPROVED

Raises a warning when patterns are unintentionally included in a set.

— Thin one-line description, no mechanism v1.20.0

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Mend.io Mend Container

Feedback ⓘ 1 RELEASE · 2026-08-23

NOTES ↗

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend Container's biggest addition this window is an AI Bill of Materials report for AI entity inventories, alongside new Chainguard hardened-image support, account-level global workflows, and several Renovate configuration and onboarding refinements.

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

01 **AI Bill of Materials (AI-BOM) report** NEW 70

Generates a comprehensive inventory of detected AI entities — including models, system prompts, agent configurations, tools, and agents — exportable via the Mend Platform reporting interface and API in `CycloneDX 1.7` and `SPDX 3.0.1` formats, across organization, application, and project scopes.

— Names formats and scopes but no exact endpoint path product docs

02 **Renovate config additions: overrideDescription and devcontainer patterns**

NEW 65

Adds `overrideDescription` option to Renovate config, allowing custom description overrides per dependency update, and adds folder pattern support to `managerFilePatterns` for the `devcontainer` manager, broadening detection of dev container configuration files.

— Names exact config keys a reader can set directly product docs

03 **Account-level global workflows with API support** NEW 60

Introduces Account-Level (Global) Workflows, letting administrators define workflows centrally and propagate them to selected organizations, with controls over whether org-level admins can enable or disable them locally. Adds comprehensive API support for managing global workflows.

— Explains propagation and control mechanism but no named endpoints product docs

THINNER COVERAGE BELOW

04 **Chainguard support in hardened image detection** NEW 55

Adds Chainguard as a supported source in hardened image detection, incorporating Chainguard-specific vulnerability and VEX data, and detects Chainguard image layers and base images within scanned containers. Chainguard VEX status and branding are shown directly in the risk factors columns across the UI for clearer posture insights on Chainguard-based images and findings.

— Describes mechanism and UI surface but no config/API detail

Version 26.8.1 (23-August-2026)

05 **Administration sidebar restructure** IMPROVED 55

Updates the Administration page sidebar with a categorized, collapsible navigation structure, including a new dedicated AI Usage tab under an AI category and sub-headers for AI, Code, and Dependencies within Engine Settings.

— Names exact nav elements, gives clear UI navigation path product docs

06 **Renovate onboarding UI improvements** IMPROVED 30

Onboarding summary view now surfaces the What to Expect section first, improving first-run clarity for new repositories, and onboarding documentation clarifies that security PRs do not count against PR limits.

— Thin, informational UI and docs changes with no mechanism product docs

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Detection Engineering

Tenzir

Feedback ⓘ 1 RELEASE · 2026-08-24 CHANGELOG ↗

Tenzir is a data pipeline platform that ingests, transforms, and analyzes security telemetry and logs for threat detection.

> Tenzir shipped parallel pipeline execution across the node and added RELP transport support for Syslog ingestion.

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

01 **Syslog ingestion over RELP** NEW 35

Tenzir Node v6.12.0 adds Syslog ingestion over RELP (Reliable Event Logging Protocol).

— Names the protocol but no config keys or usage steps given changelog-20260824-a692e9f1

02 **Parallel pipeline execution across the node** NEW 30

Tenzir Node v6.13.0 supports parallel pipeline execution across the node, enabling concurrent pipeline runs.

— States the capability but no mechanism or config detail changelog-20260824-a692e9f1

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

Yeti

Feedback ⓘ 1 RELEASE · 2026-08-24 NOTES ↗

Your Everyday Threat Intelligence

> Yeti 2.7.0 adds a dynamic endpoint for discovering creatable object types and reworks global search to group results by type with optional scoping for semantic search.

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

01 **Object-type discovery endpoint** NEW 75

A new `GET /system/types` endpoint returns a dynamic list of every creatable object type available in the Yeti instance, useful for scripting bulk ingestion or building type-aware integrations before you know the schema.

Discover every object type your Yeti instance supports — useful before scripting bulk ingestion or building type-aware integrations.

```
$ curl -s -H 'Authorization: Bearer <token>' https://<yeti-host>/api/v2/system/types | jq .
```

— Named endpoint with runnable curl example, but no schema detail 2.7.0

THINNER COVERAGE BELOW

02 **Bucketed and scopeable global search** IMPROVED 40

Global search results are now bucketed by type instead of returned as one merged, unranked list, and semantic search can be scoped to a single object type so it no longer crowds out other type results.

— Describes behavior change but no UI path or config surface named 2.7.0

WAS THIS USEFUL? 👍 👎

◆ SIEM

Sumo Logic

Feedback ⓘ 1 RELEASE · 2026-08-24 BLOG ↗

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

> Sumo Logic changed how the Save to Index alert type for scheduled searches stores results, removing the per-run result cap and altering how aggregate query fields are persisted.

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

01 Aggregate results no longer populate `_raw` field

BREAKING

88

For scheduled searches using the Save to Index alert type with aggregate queries, the `_raw` (Message) field is now empty for results saved to a `ScheduledSearchView`; all values remain accessible in their individual named fields (e.g. `_count`, `batch`, `parsedfield`). Any downstream query that uses `parse` against `_raw`, searches plain-text keywords from the message body, or reads the Message column to get field values will break and must be updated to reference named fields directly.

— Names exact fields and gives a clear migration path.

Changes to the Save to Index Alert Type…

02 Unlimited results for Save to Index scheduled searches

65

BREAKING

Removes the 512-result-per-run cap for scheduled searches using the Save to Index alert type, so every result returned by a run is now saved to the view. Searches that run frequently (e.g. every 15 minutes) without a `limit` operator may now save significantly more data per run than before.

— Names the alert type and cap removed, but no config example.

Changes to the Save to Index Alert Type…

└──▷ **BREAKING ON UPGRADE**

! For scheduled searches using the Save to Index alert type with aggregate queries, the `_raw` (Message) field is now empty — any downstream query that uses `parse` against `_raw`, searches plain-text keywords from the message body, or reads the Message column to get field values will break and must be updated to reference named fields directly.

! The 512-result-per-run limit for Save to Index scheduled searches is removed; searches that run frequently (e.g. every 15 minutes) without a `limit` operator may now save significantly more data per run than before.

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Trend Vision One

Feedback ⓘ 1 RELEASE · 2026-08-24 BLOG ↗

Trend Micro's unified security platform providing threat intelligence, endpoint protection, and attack surface visibility across cloud and on-premises environments.

> Trend Vision One's Zero Trust Secure Access On-premises Gateway 1.0.92 adds identity tracking for non-UPN users and expands DLP/AI detection log context tenfold.

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

01 **Larger DLP and AI detection log snippets** IMPROVED 60

Maximum content snippet recorded in DLP and AI detection logs increases from 100 bytes to 1,000 bytes, providing substantially more context per log entry.

— Concrete before/after limits but no action step

Zero Trust Secure Access On-premises Ga…

THINNER COVERAGE BELOW

02 **Non-UPN support in authenticated user header** IMPROVED 55

The gateway now supports non-UPN values in the `X-Authenticated-User` header and records them in traffic logs, enabling identity tracking for users whose identities are not expressed as UPNs.

— Names exact header but no config steps Zero Trust Secure Access On-premises Ga…

WAS THIS USEFUL? 👍 👎

◆ Security Data Fabric & Federated Search

Vega

Feedback ⓘ snapshot-20260824 NOTES ↗

Vega is a decentralized protocol for derivatives trading that enables peer-to-peer trading of futures and options on a blockchain.

Vega launches Detection Skills, an open standard for post-match triage, investigation, and optimization built on Anthropic's Agent Skills format.

└──▷ HOW TO FIND IT

Export a spec-compliant Detection Skill as YAML from the detectionskills.io sandbox to review or contribute the skill to the community library.

📍 In the detectionskills.io sandbox: build a detection, attach a triage or investigation skill from the library, preview the verdict, then click Export to download a spec-compliant YAML file. Submit it via the linked GitHub repository to publish it to the community library.

Launches the Detection Skills open standard at detectionskills.io, built on Anthropic's Agent Skills format, for encoding triage, investigation, and detection-optimization logic as versioned, shareable YAML skills.

Integrates Detection Skills into the Vega Cyber Defense Platform via a detection notebook workflow: compose detection logic, attach skills for triage/investigation/optimization, and receive tuning proposals with attached reasoning for engineer approval.

Adds an optimization loop that writes approved verdicts back into the detection rule, incrementally sharpening coverage with each alert fire.

Enables agentic detection and triage for emerging threat landscapes including dangerous AI model activity, with skills scoped to specific use cases rather than relying on a single catch-all agent.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

DNSFilter

Feedback ⓘ 1 RELEASE · 2026-08-24 CHANGELOG ↗

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

> DNSFilter shipped SecureTransit, a new VPN-layer encryption policy for DNS traffic, alongside a full redesign of the DNSFilter One Agent and several dashboard usability changes.

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

01 SecureTransit encrypted VPN-layer traffic policy NEW

88

A new SecureTransit feature enforces DNS-layer traffic encryption through a DNSFilter-managed secure gateway, using either WireGuard or IKEv2 protocols. Policy can be set per-organization or per-device to Always On, Manual, or Disabled from the existing DNS filtering dashboard, and it blocks location trackers, mail trackers, data brokers, and ad networks on-path before data leaves the device on any network. It is available as a per-device add-on with a 14-day free trial for existing customers, requiring no client-side credential setup.

Enforce always-on encrypted transit for a high-risk device group without requiring employees to configure anything.

> 📍 In the DNSFilter dashboard, go to the policy settings for the target organization or device, locate SecureTransit, set the mode to `Always On`, choose WireGuard or IKEv2 as the protocol, and save. Credentials and gateway connections are provisioned server-side automatically.

— Names modes, protocols and rollout mechanics but no API/CLI surface.

changelog-20260824-02df8de5

02 **Redesigned DNSFilter One Agent UI** IMPROVED 70

The DNSFilter One Agent (Windows) replaces the tray right-click menu with a full-window UI themed to system light or dark mode. Its Filtering panel shows protection state, filtering mode, last sync time, and an activity view of blocked and allowed queries over the past hour. Its SecureTransit panel (visible when SecureTransit is enabled) shows connection status, connected server on a map, region, protocol, session uptime, data transferred, and Connect/Disconnect controls. Its Settings panel consolidates version, hostname, diagnostics, and logs in one place.

— Names every panel and field but is a UI redesign, no exact navigation steps.

changelog-20260824-02df8de5

THINNER COVERAGE BELOW

03 **Consolidated Query Log filter panel** IMPROVED 40

Query Log filters have been consolidated into a single top-level panel with a unified Apply button, eliminating the need to set filters across multiple locations.

— Describes the change but gives no field names or exact UI path.

changelog-20260824-02df8de5

04 **Removal of Dashboard 'Reset to Default' action** BREAKING 40

The destructive Reset to Default option has been removed from the Dashboard Actions menu; any workflow relying on it to reset dashboard layout will no longer find this control.

— Clear before/after but names only a menu item, not a config surface.

changelog-20260824-02df8de5

05 **Dashboard widget placement and view improvements** IMPROVED 35

Dashboard widget placement now drops newly added widgets into the next available grid slot without overlapping or displacing existing widgets, and a persistent time range indicator remains visible while scrolling or switching dashboard views.

— Two thin dashboard UX tweaks with no further mechanism detail.

changelog-20260824-02df8de5

└──▷ BREAKING ON UPGRADE

! The Reset to Default option has been removed from the Dashboard Actions menu — any workflow relying on it to reset dashboard layout will no longer find this control.

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

Auth0

Feedback ⓘ 1 RELEASE · 2026-08-24 CHANGELOG ↗

Secure users, AI agents, and more with Auth0, an easy-to-implement, scalable, and adaptable authentication and authorization platform.

> Auth0 introduces Custom Rate Limits in Early Access, letting teams self-service throttle Authentication API consumption per client with either blocking or notify-only enforcement.

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

01 Custom Rate Limit Policies for Authentication API NEW

60

Adds API-based self-service configuration of Custom Rate Limit Policies to cap Authentication API OAuth request consumption per individual client, all third-party apps, or CIMD apps. Policies support configurable enforcement modes: block requests outright, or trigger non-blocking notifications for safer, gradual rollout.

. . . .

— Names scope and modes but no API endpoint or config key `changelog-20260824-f389ba09`

WAS THIS USEFUL? 👍 👎

Ping Identity

Feedback ⓘ 1 RELEASE · 2026-08-24 CHANGELOG ↗

Read docs, explore use cases, learn best practices

> Ping Identity's PingOne AIC rapid channel shipped a batch of admin console refinements this window, including ESV support for connector server names, clearer script error feedback, faster identity and job editing workflows, and a reorganized navigation structure.

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

01 **Reorganized navigation for verification, attestation and security settings**

IMPROVED 60

Moves the Identity Verification page under Integrations, Android Key Attestation under Authentication Methods, and Security Questions under Authentication in the admin console navigation.

– Names all three relocated pages and their new locations changelog-20260824-6e6a101a

THINNER COVERAGE BELOW

02 **ESV support for connector server name** NEW 55

The New Connector Server modal now supports using an ESV (Environment Secret/Variable) to set the connector server name.

– Names exact modal and field, lacks further mechanism changelog-20260824-6e6a101a

03 **Script error visibility for ESV references** IMPROVED 45

The script editor now surfaces script errors directly in the editor when scripts reference environment ESVs incorrectly.

– Explains what changed, no config detail given changelog-20260824-6e6a101a

04 **Faster consecutive identity creation** IMPROVED 40

Users can now create another identity immediately after creating one, without closing the creation modal.

– Clear workflow change but no further scope changelog-20260824-6e6a101a

05 **Edit future-scheduled jobs to start sooner** IMPROVED 40

Supports editing a job that is scheduled to run in the future so that it starts sooner than originally planned.

— Names the capability but no mechanism detail changelog-20260824-6e6a101a

06 **Modal and form usability improvements** IMPROVED 30

Modals can now be closed with the Escape key, and form submissions now clearly highlight fields containing errors.

— Two minor UI polish items, thinly described changelog-20260824-6e6a101a

WAS THIS USEFUL? 👍 👎

iDenfy

Feedback

1 RELEASE · SEEN 2026-08-24

NOTES ↗

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

> iDenfy's headline addition this window is a standalone Bank Card Verification flow running in a dedicated PCI-DSS v4.0.1 certified environment, shipped alongside Persian (Farsi) RTL identity verification, Brazil Digital CNH support, and a cluster of smaller KYB automation, data-field, and dashboard improvements.

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

01 **Standalone Bank Card Verification flow** NEW 78

Bank Card Verification can now run as a standalone flow, independently of identity verification, or as an additional step inside an existing KYC flow, confirming the card used at onboarding belongs to its holder. The standalone flow is processed in a dedicated PCI-DSS v4.0.1 certified environment and includes consent and capture screens, retry-attempt tracking, dual session clocks, and end-user result screens.

— Names environment and components but no exact API/flag snapshot-20260824

02 **Full locale code reference for 37 languages** NEW 60

Publishes a full locale code reference covering all 37 supported languages, including both Latin and non-Latin scripts, for use in KYC and KYB verification flows.

— Concrete language count, reference usable directly product docs

THINNER COVERAGE BELOW

03 **Risk Assessment PDF export** NEW 55

Dashboard users can now export a Risk Assessment as a PDF from any KYC or KYB record for offline review or audit evidence.

Export a Risk Assessment as a PDF for offline review or audit evidence from a KYC record.

📍 In the dashboard, open any KYC or KYB record › locate the Risk Assessment section › click Export PDF.

— Exact UI navigation path provided in example product docs

04 **Persian (Farsi) RTL identity verification** NEW 55

Identity verification now supports Persian (Farsi) with a full right-to-left (RTL) layout and automatic photo capture on the selfie step.

— Describes layout and capture behaviour, no config surface `snapshot-20260824`

05 **No-further-shareholders declaration in KYB ownership chains** NEW 55

KYB ownership chains can now terminate at a company declared to have no further shareholders, closing open-ended UBO (ultimate beneficial owner) chains.

— Explains mechanism and purpose but no UI/API detail `snapshot-20260824`

06 **VAT Number, EIN, and TIN fields in KYB** NEW 50

KYB workflows now include dedicated tax identification fields — `VAT Number`, `EIN`, and `TIN` — for capturing business tax identifiers.

— Names exact fields but no workflow mechanism `product docs`

07 **Brazil Digital CNH document support** NEW 45

Adds Brazil's Digital CNH (digital driver's license) as a supported identity document type for identity verification.

— Names document type but no flow detail `product docs`

08 **API endpoint to re-run KYB automation** NEW 43

A new API endpoint lets you programmatically re-trigger automated checks on existing KYB records, enabling re-running KYB automation without recreating a record.

— Endpoint exists but no exact path or method given `product docs`

09 **External Reference field in KYC reports** NEW 42

KYC verification reports now include an `External Reference` field for linking verifications to external systems.

— Names field but no usage detail `product docs`

10 **Automated reminders in KYB Verify Later** IMPROVED 40

KYB Verify Later now sends automated IDV reminders to beneficial owners to prompt them to complete verification.

— Describes behaviour but no trigger schedule or config `product docs`

11 **Dedicated branding color for primary buttons** IMPROVED 40

Primary buttons now support a dedicated branding color, separate from the general brand color configuration.

— Names the setting but no config key or path `snapshot-20260824`

12 **Spelling variation matching in AI reviewer** IMPROVED

30

The AI reviewer now matches spelling variations in name/entity review, improving detection of near-matches during automated review.

— No mechanism or examples of matching logic given product docs

13 **Open dashboard records in new tab** IMPROVED 20

Dashboard records can now be opened in a new browser tab.

— Minor UI change with no further detail product docs

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

Mend.io Mend AI

Feedback ⓘ 1 RELEASE · 2026-08-24 NOTES ↗

Traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend AI's biggest addition this window is an AI Bill of Materials (AI-BOM) report for inventorying AI entities, alongside account-level global workflows with API management, Chainguard support in hardened image detection, a breaking Administration sidebar redesign, and a batch of Renovate configuration and onboarding tweaks.

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

01 **AI Bill of Materials (AI-BOM) report** NEW 78

New AI-BOM report available via the Mend Platform reporting interface and API, generating a metadata-only inventory of detected AI entities — models, system prompts, agent configurations, tools, and agents — scoped at organization, application, and project levels. Exports support the industry-standard `CycloneDX 1.7` and `SPDX 3.0.1` formats for interoperability with existing SBOM toolchains and compliance workflows.

— Names formats and scopes but no exact API endpoint (24-August-2026)

02 **Chainguard support in hardened image detection** NEW 70

Chainguard is now a supported source in hardened image detection, incorporating Chainguard-specific vulnerability data, VEX information, and base image/layer detection. Chainguard VEX status and branding are surfaced directly in the risk factors columns across the UI for Chainguard-based images and findings.

— Names the integration and UI surface but no config steps product docs

03 **Renovate config, manager coverage and onboarding tweaks**

IMPROVED 67

Mend Renovate adds the `overrideDescription` config option to set custom descriptions on dependency update PRs, and adds folder pattern support to `managerFilePatterns` for the `devcontainer` manager to broaden file detection. The onboarding summary view now shows What to Expect first and clarifies that security PRs do not count against PR limits, and the Gradle manager now links to Dependency Verification documentation.

Override the auto-generated description on a Renovate dependency update PR using the new `overrideDescription` config option.

```json
{
  "overrideDescription": "Managed dependency update — reviewed by platform team"
}
```

— Names config key with runnable example, rest are thin UI notes `product docs`

04 **Account-level global workflows** NEW 65

Administrators can now define workflows centrally at the account level and propagate them to selected organizations, with controls over whether org-level admins can enable or disable them locally. Comprehensive API support was added for managing these global workflows.

— Describes mechanism but no concrete API paths given `product docs`

05 **Administration sidebar redesign moves AI Usage settings** 60

BREAKING

The Administration page sidebar was redesigned with a categorized, collapsible navigation structure, adding a dedicated `AI Usage` tab under a new AI category and sub-headers for AI, Code, and Dependencies within Engine Settings. This is a breaking change: AI Usage settings moved from the General tab to the new dedicated tab, so any documentation or runbooks pointing to the General tab need updating.

— Clear UI path given but no config/API detail `product docs`

└──▷ **BREAKING ON UPGRADE**

! AI Usage settings have been moved from the General tab to a dedicated `AI Usage` tab under the new AI category in the Administration sidebar — any documentation or runbooks pointing to the General tab for AI Usage settings will need to be updated.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

goshs

Feedback ⓘ 1 RELEASE · 2026-08-24 NOTES ↗

Feature-rich single-binary file server for red teamers and developers. HTTP/S · WebDAV · FTP/SFTP · SMB · LDAP/S · NTLM hash capture · DNS/SMTP callbacks · TLS · Auth · Share links.

> goshs v2.1.6 replaces the old shared clipboard with a full persistent team chat (Markdown, ~1800 emoji, reactions, editing, image paste, file upload) synced across the web UI and TUI, adds an upload size cap, and closes several read-only/upload-only and ACL/auth bypasses across SMB, TFTP, HTTP and WebDAV.

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

01 **Persistent team chat across web UI and TUI** NEW 95

A new live team chat synchronized over a WebSocket connection replaces the old non-persistent shared clipboard in both the web UI and the `--tui` dashboard (TUI authors as `tui@<host>`). Messages render as Markdown with the full `:shortcode:` emoji set (~1800 emoji from the Mattermost catalog), composer autosuggest, collapsible code blocks (collapsed past 10 lines), emoji reactions with a who-reacted tooltip, in-place editing of own messages (press `↑` in the composer to recall and cycle previous messages, edits marked (edited)), image paste (inlined as base64 by default), file upload via a `POST /?chatUpload` endpoint (files land in `.goshs-chat/`, hidden from directory listing, respecting `--read-only`), and opt-in desktop Web Notifications for messages received while the tab is hidden. Chat can be disabled entirely with the `-nc` / `--no-chat` flag or `no_chat` config key (this replaces the old `--no-clipboard` flag, breaking any scripts that used it); the full chat log — messages, edit flags, per-emoji reaction authors — can be persisted to `<webroot>/.goshs-chat/chat.json` via `-pc` / `--persist-chat` (`persist_chat` config key) and restored on restart, with pasted images additionally written to disk via `-pci` / `--persist-chat-images` (`persist_chat_images` config key) instead of being inlined.

Persist the chat log and pasted images to disk so the conversation survives a goshs restart — useful across a long engagement.

```
$ goshs --persist-chat --persist-chat-images
```

Disable the team chat entirely when you want a clean, read-only file-sharing session without collaboration features.

```
$ goshs --no-chat
```

Configure chat persistence options in the goshs config file instead of passing flags each run.

```json
{
  "no_chat": false,
  "persist_chat": true,
  "persist_chat_images": true
}
```

Serve files without exposing the team chat — useful when sharing with untrusted recipients or in restricted environments.

```
$ goshs --no-chat
```

Disable chat entirely and avoid persisting any chat data when running goshs as a clean file-sharing server.

```yaml
no_chat: true
persist_chat: false
persist_chat_images: false
```

Run a persistent session that retains all chat messages and pasted images across restarts for later review.

```
$ goshs --persist-chat --persist-chat-images
```

Persist team chat history and pasted images across server restarts during a long engagement.

```
$ goshs --persist-chat --persist-chat-images
```

Run a read-only file server with chat disabled when you do not want any collaboration surface exposed.

```
$ goshs --read-only --no-chat
```

— Names every flag, config key, endpoint and storage path involved v2.1.6

02 **Configurable upload size limit** NEW 70

Adds the `-mu` / `--max-upload` flag to cap file upload size in bytes, defaulting to `0` (unlimited).

Cap uploads at 100 MB in a shared-session deployment so users cannot fill disk with large files.

```
$ goshs --max-upload 104857600
```

— Exact flag and default given, but limited context on error behavior product docs

03 **Read-only/upload-only write-path enforcement hardened** 70

BREAKING

`--no-delete`, `--upload-only` and `--read-only` are now enforced across SMB, TFTP, HTTP and WebDAV write paths: overwrite, in-place write, truncate, and rename/move of pre-existing files are now refused as deletion-class operations, closing gaps where these were previously permitted.

— Names the flags and protocols but gives no reproduction command v2.1.6

04 **WebDAV LOCK/UNLOCK blocked under restrictive modes** IMPROVED 65

WebDAV `LOCK` / `UNLOCK` operations are now blocked by `webdavGuard` when `--read-only` or `--upload-only` is set, preventing lock-null empty file creation that previously bypassed those modes.

— Names the guard and methods but no runnable reproduction v2.1.6

05 **ACL resolution merges .goshs files up to webroot** IMPROVED 65

`findEffectiveACL` now merges `.goshs` files up to the webroot: the nearest ancestor that sets `Auth` wins, and block lists are unioned, preventing a block-only child `.goshs` file from erasing a parent directory's auth requirement.

— Names the function and merge rule but no example config shown v2.1.6

THINNER COVERAGE BELOW

06 **Collaborator feed strips Authorization header** IMPROVED 50

The collaborator feed now unconditionally strips the `Authorization` header, alongside the CSRF token, at every call site, preventing per-directory ACL credentials from leaking to unauthenticated watchers.

— Clear fix described but no way to verify or invoke it directly v2.1.6

└──▷ BREAKING ON UPGRADE

! The `--no-clipboard` flag is replaced by `--no-chat` (`-nc`); any scripts or configs using `--no-clipboard` will break on upgrade.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 24, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue