THE CYBER TOOLCHAIN

NO. 048

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED AUGUST 17, 2026 · EVERY DAY

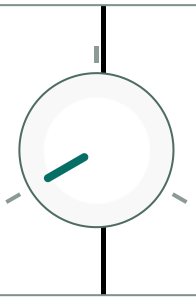
The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 26 tools

OFFENSIVE SECURITY

vim ? help

◆ Wireless & RF

SensePost hostapd-mana

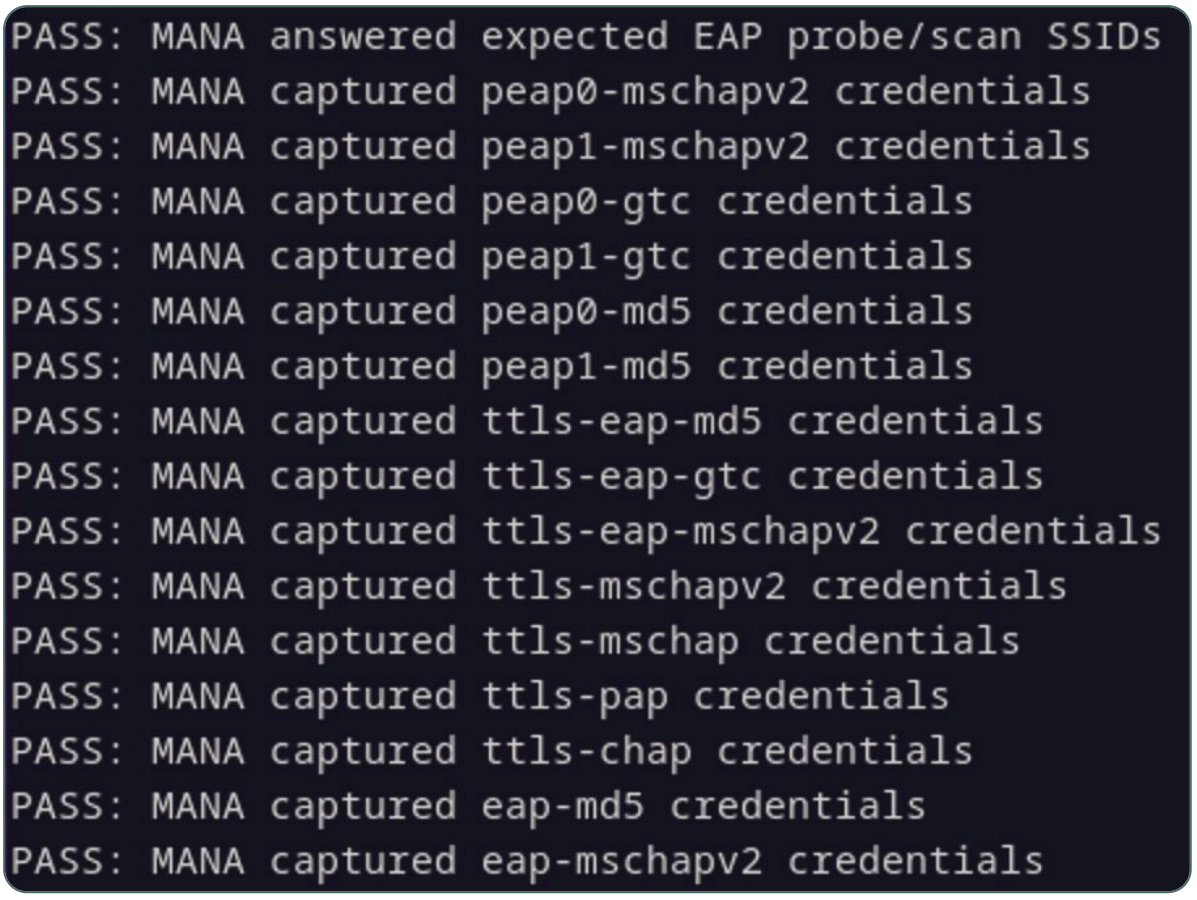
Feedback ⓘ 2.12 NOTES ↗

SensePost's modified hostapd for wifi attacks.

hostapd-mana 2.12 ports to hostapd 2.12 with full 802.11be 6 GHz support and all 16 EAP credential-intercept modes.

└──▷ GET THIS VERSION

```
$ git clone --branch 2.12 https://github.com/sensepost/hostapd-mana.git
# already have the repo? check out this version:
$ git checkout 2.12
```



Supports 802.11be (Wi-Fi 7) and 6 GHz band operation, enabling rogue AP and credential-intercept testing against modern 802.11be clients.

Maintains all 16 EAP mode interceptions (credential capture and credential-material capture) on 802.11be 6 GHz networks.

WAS THIS USEFUL?  

APPLICATION SECURITY

◆ Web Application Security

Invicti

Feedback ⓘ 1 RELEASE · 2026-08-17 CHANGELOG ↗

Invicti is an automated web application security scanning platform that identifies vulnerabilities like SQL injection and XSS through dynamic and interactive testing.

> Invicti's latest release adds HashiCorp Vault-backed secrets for scan authentication, a dedicated API scan profile, and finer-grained control over scan speed, alongside improvements to gRPC imports, Login Sequence Recorder reporting, and IDOR/BOLA credential limits.

└──▷ WHAT SHIPPED · 7 FEATURES most completely described first ? what's the number?

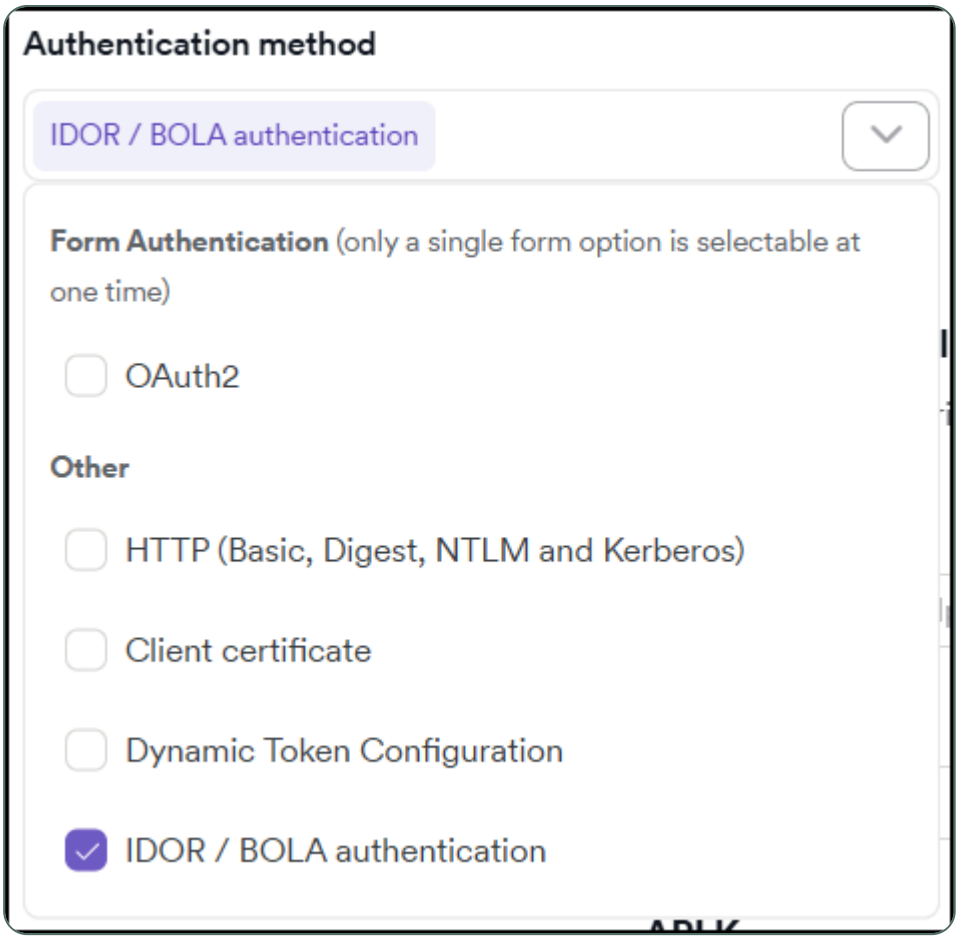
01 **Custom scan speed control** NEW 65

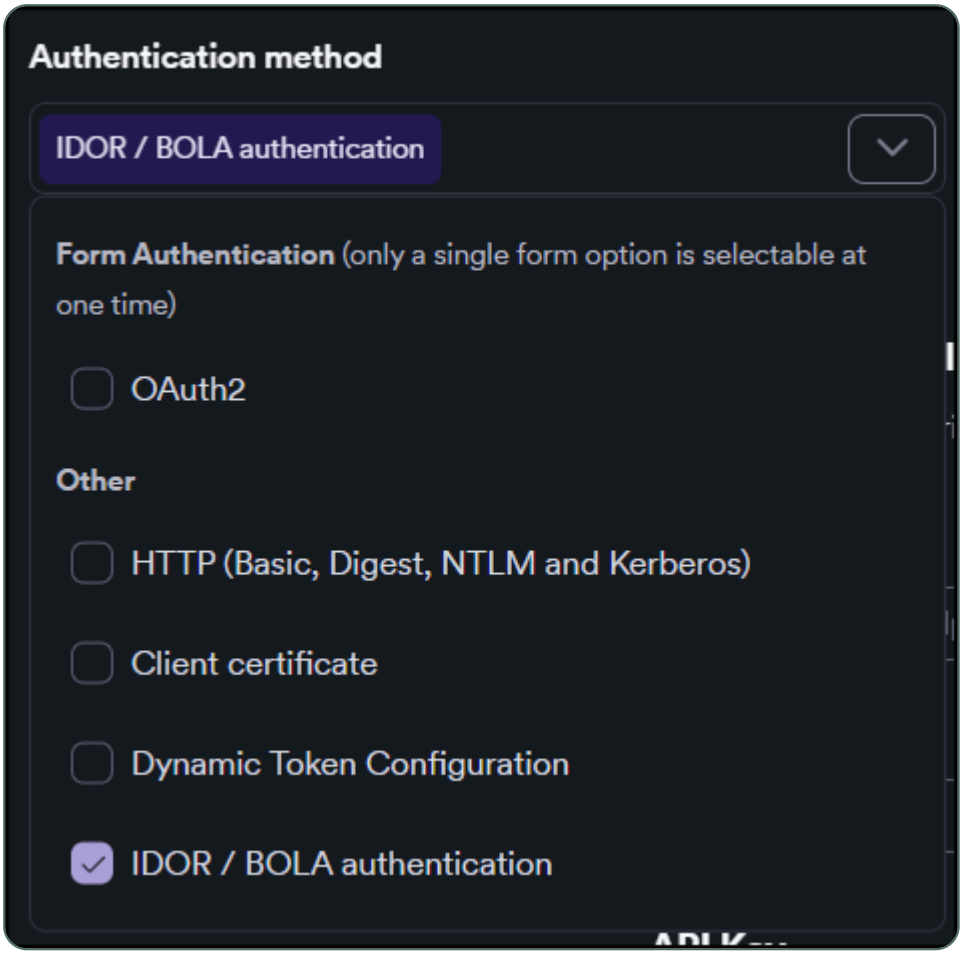
Adds a new Custom scan speed option in scan configuration that lets users set the number of concurrent requests and the throttling delay for precise throughput control.

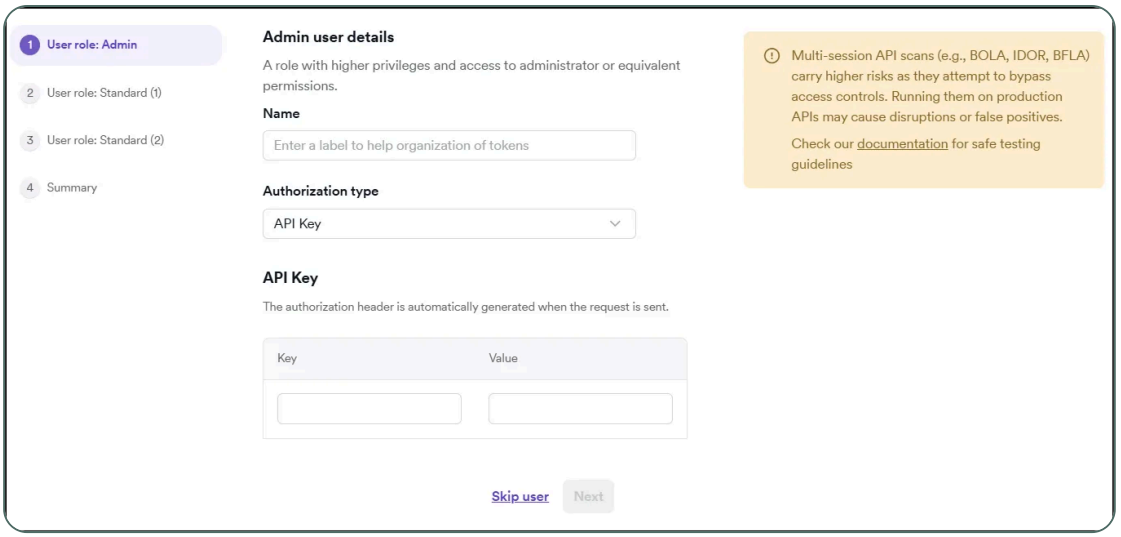
— Names exact configurable parameters and where to set them. changelog-20260817-ad34ccb5

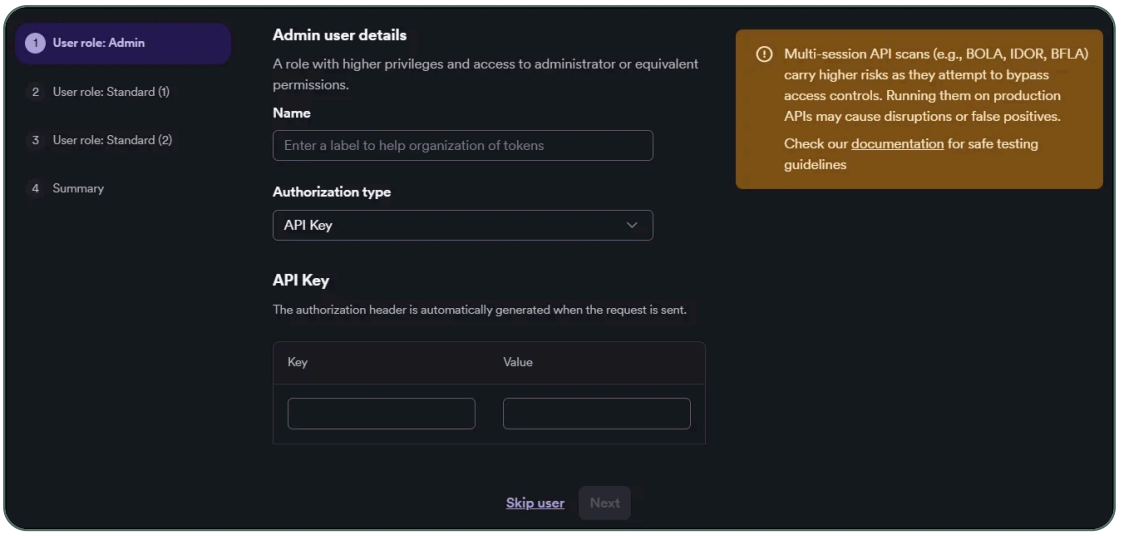
02 **Expanded IDOR/BOLA credential character limit** IMPROVED 65

Increases the character limit for authentication values in IDOR/BOLA credentials from 1,024 to 4,096 characters, accommodating long JWT Bearer Tokens.


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


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





— Gives exact before/after limits and use case. `changelog-20260817-ad34ccb5`

03 Full HTTP traffic logging in Login Sequence Recorder IMPROVED

60

Expands Login Sequence Recorder (LSR) reports to include the full HTTP request and response for each recorded step, with automatic obfuscation of sensitive tokens in headers and bodies.

— Explains mechanism and scope but no report location detail. `changelog-20260817-ad34ccb5`

THINNER COVERAGE BELOW

04 HashiCorp Vault integration for scan credentials NEW

52

Adds HashiCorp Vault integration with Invicti Platform's Secrets Manager, enabling credentials to be retrieved directly from Vault when configuring scan authentication.

— Names the integration and mechanism but not setup steps. `changelog-20260817-ad34ccb5`

05 Multi-file gRPC ZIP upload NEW

47

Adds support for uploading multiple gRPC proto file definitions as a single ZIP archive, eliminating the need to import multi-file gRPC service definitions one by one.

— Describes the change but no exact upload path or size limit.

changelog-20260817-ad34ccb5

06 **Secrets access during LSR recording** IMPROVED 45

Secrets configured for a target are now accessible to the Login Sequence Recorder (LSR) during recording, so stored credentials can be used instead of being entered manually.

— States behavior change but no config path given. changelog-20260817-ad34ccb5

07 **Dedicated API scan profile** NEW 30

Adds a new dedicated API scan profile that is applied by default to all new API targets, intended to provide comprehensive API vulnerability coverage.

— Bare description of a default profile with no configuration detail.

changelog-20260817-ad34ccb5

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

Cloudsmith

Feedback ⓘ 1 RELEASE · 2026-08-17 CHANGELOG ↗

Cloudsmith is a cloud-based software supply chain platform for securely managing and distributing software packages and artifacts.

> Cloudsmith reached general availability for policy-as-code management and continuous risk detection, while switching its vulnerability data source from Trivy to OSV.dev and improving the policy editor's authoring experience.

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

01 **Policy management GA across web app, API, Terraform** NEW

60

Policy management is now generally available across the web app, API, and Terraform provider, enabling policy-as-code enforcement rules across the software supply chain.

— Names three surfaces but no concrete rule syntax or endpoint given

changelog-20260817-a2e2ac1d

THINNER COVERAGE BELOW

02 **Inline Rego linting and autocomplete in policy editor**

IMPROVED

55

The policy editor now provides inline Rego error flagging and schema-field autocomplete as you type, surfacing mistakes before saving.

— Names Rego and autocomplete but only a UI path, not a command

changelog-20260817-a2e2ac1d

03 **Continuous risk detection GA** NEW

50

Continuous risk detection is now generally available, automatically checking every package in a workspace against known vulnerabilities and malicious packages with no scheduled or manual rescans required.

— Explains automatic mechanism but no config or trigger to act on

changelog-20260817-a2e2ac1d

04 **OSV.dev replaces Trivy as vulnerability data source** IMPROVED

40

OSV.dev now replaces Trivy as the vulnerability data source shown in the web app and API for risk detection.

— Informational data-source swap with no user action required changelog-20260817-a2e2ac1d

WAS THIS USEFUL?  

GitHub

Feedback

3 RELEASES · 2026-08-14

BLOG ↗

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

> GitHub shipped OAuth app security upgrades — expiring tokens with refresh and support for multiple, wildcard redirect URIs — alongside a broad Copilot update wave covering Grok 4.6 and other new models, GA cross-surface plugins, new CLI task/planning/rewind commands, JetBrains BYOK and memory, and VS Code model switching.

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

01 Expiring tokens and refresh flow for OAuth apps NEW

88

OAuth apps can include the `offline_access` scope in authentication requests to opt into short-lived access tokens (8-hour lifetime) paired with 6-month refresh tokens. Registrations can also be set to always issue short-lived tokens, forcing even old clients onto the refresh flow; the behavior is enabled by default for all newly created OAuth apps and can be disabled while updating an incompatible SDK.

Test refresh-token support in a new OAuth app flow by requesting short-lived tokens via the `offline_access` scope during user authorization.

```
$ GET https://github.com/login/oauth/authorize?client_id=
<client_id>&scope=repo%20offline_access&redirect_uri=https://app.
example.com/callback
```

— Names the scope, exact durations, and includes a runnable auth request.

Multiple redirect URIs and token refres…

02 Task, planning and rewind commands in Copilot CLI NEW

88

Copilot CLI gains a `/tasks` subcommand to manage all subagents and their tasks, supporting queuing of prompts, shell commands, and slash commands while an agent turn is running; `--plan` combined with `--mode autopilot` in headless mode (`-p`) to have the agent produce and then automatically implement a plan; and `/rewind` to restore Copilot changes without requiring git or discarding user edits. The `/app` command was also updated to preserve session and folder context when opening the Copilot app.

Roll back Copilot-generated changes mid-session without touching git history or throwing away your own edits.

```
$ /rewind
```

— Names exact runnable subcommands and flags for the CLI.

GitHub Copilot weekly releases — August…

03 **Grok 4.6 model in GitHub Copilot** NEW 71

Grok 4.6 is now selectable in the Copilot model picker across Visual Studio Code, Visual Studio, Copilot CLI, GitHub Copilot cloud agent, GitHub Copilot app, JetBrains, Xcode, and Eclipse. It's available to Copilot Pro, Pro+, Max, Business, and Enterprise SKUs at provider list pricing under usage-based billing, and Enterprise/Business admins must enable the Grok 4.6 policy in Copilot settings, which is off by default.

— Lists surfaces, SKUs, billing and admin toggle but no exact settings path.

Grok 4.6 is now available in GitHub Cop…

04 **Multiple and wildcard redirect URIs for OAuth apps** BREAKING 70

OAuth apps can now register up to 10 redirect URIs (called `callback URIs`) via a new `Add redirect URI` button in application settings, and both OAuth apps and GitHub Apps can enable per-URI wildcard matching so authorization redirects work for subdomain or subpath variants without registering each one. Apps with a single redirect URI now have wildcard matching enabled by default, a previously invisible legacy behavior that operators should explicitly disable if not needed to reduce redirect attack surface.

— Names the UI control and limits but only points to settings, no API/config key.

Multiple redirect URIs and token refres…

THINNER COVERAGE BELOW

05 **Plugin management and side chat in Copilot app** IMPROVED 58

The Copilot app now shows each installed plugin's current version and supports individual or bulk plugin updates from `Customize` or `Settings`. It also lets users open an agent's question in a side chat to discuss it before responding, while the original question waits.

Inspect and bulk-update all installed Copilot plugins from one place in the app.

📍 In the Copilot app, go to Customize (or Settings) › Plugins, review each plugin's current version, then click `Update all` to upgrade every plugin at once.

— Includes exact UI navigation steps for bulk plugin updates.

GitHub Copilot weekly releases — August…

06 **Mid-session model switching in VS Code** IMPROVED 56

VS Code 1.133 allows switching between Claude BYOK and built-in Copilot models mid-session, per turn, without leaving the Claude session.

— Names the VS Code version and models but no exact UI steps.

GitHub Copilot weekly releases — August…

07 **Agent Plugins 1.0 general availability** NEW 54

`Agent Plugins 1.0` is now generally available, letting a plugin built once run across VS Code, Copilot CLI, the GitHub Copilot SDK, and the GitHub Copilot app.

— Names the surfaces and GA status but no setup steps given.

GitHub Copilot weekly releases — August…

08 **Ollama BYOK support in JetBrains** NEW 48

GitHub Copilot for JetBrains now supports Ollama as a BYOK (bring your own key) provider, enabling use of local Ollama models.

— Names the provider and IDE but no configuration steps.

GitHub Copilot weekly releases — August…

09 **New Copilot models: Kimi K3 and MAI-Code-1.1-Flash** NEW 43

Kimi K3 rolled out to Copilot Pro, Pro+, Max, Business, and Enterprise plans, and MAI-Code-1.1-Flash rolled out with native image understanding and improvements to coding quality, instruction following, tool use, and performance.

— States availability and plan tiers but no usage instructions.

GitHub Copilot weekly releases — August…

10 **Cross-session memory in Copilot for JetBrains** NEW 32

Adds Copilot memory in JetBrains to persist useful context across agent chat sessions.

— Bare description of the capability with no mechanism detail.

GitHub Copilot weekly releases — August…

└──▷ **BREAKING ON UPGRADE**

! Apps with only one registered redirect URI have wildcard matching enabled by default as a now-visible legacy behavior; operators who do not need it should explicitly disable it in application settings to reduce redirect attack surface.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Malware Analysis

CAPEv2

Feedback ⓘ changes since 2026-08-15 CODE ↗

Malware Configuration And Payload Extraction

CAPEv2 Distributed REST API migrated to FastAPI/Uvicorn with self-healing DB connections and expanded admin CLI

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-08-15
https://github.com/kevoreilly/CAPEv2.git
# already have the repo? check out this version:
$ git checkout commits-2026-08-15
```

Migrates the Distributed REST API in `utils/dist.py` from Flask/Flask-RESTful to FastAPI and Uvicorn, with type-safe Pydantic JSON schemas replacing Flask-SQLAlchemy and python-multipart.

Adds a restart_db_connection() helper and `SessionWrapper` in `utils/dist.py` that automatically disposes and recreates the SQLAlchemy connection pool when a `TimeoutError` or `QueuePool` limit is hit.

Expands `utils/dist.py` into a fully-featured administrative CLI tool with grouped command sets: Daemon Options, Cluster Management, VM Maintenance, and GCS/Sync — adding subcommands to list, register, modify, and view cluster status from the command line.

└──▷ BREAKING ON UPGRADE

! The Distributed CAPE REST API (`utils/dist.py`) now requires FastAPI and Uvicorn instead of Flask, Flask-RESTful, Flask-SQLAlchemy, and python-multipart; these dependencies have been removed from `pyproject.toml` and must be replaced before upgrading.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Sophos Email Security

Feedback ⓘ 1 RELEASE · 2026-08-11

NOTES ↗

Sophos Email Security protects organizations from email-based threats including malware, phishing, and spam through advanced threat detection and filtering.

> Sophos Email Security 2026.32 improves Time-of-Click URL protection with exportable URL lists and more nuanced custom messaging for unverified links.

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

01 **CSV/PDF export of message URL lists** NEW 67

From the URLs tab in Message Details, admins can now export the list of URLs found in a message as CSV or PDF, including basic message metadata to help identify the source message.

– Names exact UI location and export formats, no example given

2026.32Released August 11, 2026

THINNER COVERAGE BELOW

02 **Custom messages for unverified Time-of-Click links** IMPROVED 58

Custom block and warning messages for unverified Time-of-Click (ToC) links can now be configured separately from those shown for known risky URLs, allowing less alarming messaging for links that are unverified but not confirmed malicious.

– Explains behavior change but no exact config path given 2026.32Released August 11, 2026

WAS THIS USEFUL? 👍 👎

Sophos DNS Protection

Feedback

1 RELEASE · 2026-08-05

NOTES ↗

Sophos DNS Protection is a security service that blocks malicious websites and threats by filtering DNS queries at the network level.

> Sophos DNS Protection adds a dedicated Generative AI web category for granular filtering, along with a renamed category group and an inheritance rule that admins should review.

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

01 Generative AI category for filtering policies NEW

73

A new Generative AI category has been added to the Business and generative AI category group (renamed from Business-relevant site categories), letting filtering policies block or allow generative AI service websites independently of other business categories. In existing filtering policies, the new Generative AI category automatically inherits the setting of the Information technology category (e.g., if Information technology is set to Allow, Generative AI will also be Allow), so admins should review policies where Information technology is allowed if they intended to block generative AI sites.

— Names category, group rename, and inheritance rule but no UI path

2026.32Released on August 5, 2026

└──▷ **BREAKING ON UPGRADE**

! The Business-relevant site categories category group is renamed to Business and generative AI; any documentation or references using the old name will need to be updated.

! In existing filtering policies, the new Generative AI category automatically inherits the setting of the Information technology category (e.g., if Information technology is set to Allow, Generative AI will also be Allow) — review policies where Information technology is set to Allow if you intended to block generative AI sites.

WAS THIS USEFUL? 👍 👎

Sophos Access Points

Feedback

1 RELEASE · 2026-07-20

NOTES ↗

Sophos Access Points are wireless networking devices providing secure, managed WiFi connectivity with integrated threat protection for enterprise environments.

> Sophos Central 2026.29 adds WMM-EDCA traffic prioritization controls for access point profiles and strengthens the AP6 registration flow with real-time validation and a troubleshooting link.

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

01 **WMM-EDCA traffic prioritization for AP profiles** NEW

57

Adds WMM-EDCA (Wireless Multimedia - Enhanced Distributed Channel Access) traffic prioritization settings, configurable on the Advanced Wireless tab of access point profiles.

— Names exact UI tab but not mechanism details of prioritization.

Central 2026.29NewReleased on July 20, …

02 **AP6 registration validation and help improvements** IMPROVED

52

Adds real-time serial number validation during AP6 registration that surfaces format and licensing errors before registration starts, adds registration account validation that shows an error when an access point connects but is already registered to another account, and adds a Need help? link in the AP6 registration window linking to the updated troubleshooting guide.

— Describes three registration-flow checks without exact error text or UI path.

Central 2026.29NewReleased on July 20, …

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Plerion

Feedback ⓘ 1 RELEASE · SEEN 2026-08-17 NOTES ↗

Plerion is a cloud security platform that enables continuous vulnerability discovery and remediation across cloud infrastructure and applications.

> Plerion rebuilt its entire compliance framework catalog from scratch, adding CIS AWS Foundations Benchmark v7.0.0 and 15,250 new control-to-detection mappings, while promoting 18 frameworks to their latest publisher editions and retiring 23 superseded ones.

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

01 **CIS AWS Foundations Benchmark v7.0.0 support** NEW 80

Adds `CIS Amazon Web Services Foundations Benchmark v7.0.0` with all 70 recommendations mapped to Plerion detections, including six new AWS Organizations controls (centralized root access, authorization guardrails, organizational unit structure, delegated administrators) and a check for reaching AWS services over VPC endpoints, each tagged with CIS Level 1 or Level 2 profile.

– Fully specified scope and controls, but no direct link or command given

Plerion's compliance frameworks, rebuil…

02 **Full rebuild of 40 compliance frameworks** BREAKING 75

Plerion rebuilt all 40 compliance frameworks from scratch against the current detection catalog, producing 15,250 control-to-detection mappings across AWS, Azure, GCP, and now Kubernetes (29 frameworks). Because mappings were reconstructed rather than patched, compliance posture percentages will shift in both directions across all 40 rebuilt frameworks.

– Explains mechanism and impact but no remediation steps given

Plerion's compliance frameworks, rebuil…

03 **23 superseded compliance frameworks retired** DEPRECATED 68

Retires 23 superseded framework editions — including `PCI DSS 4.0`, `PCI DSS 3.2.1`, `NIST CSF v1.1`, `ISO/IEC 27001:2013`, `CIS AWS Foundations Benchmark v4.0.1`, and `FFIEC CAT` — removing them from the framework list while preserving existing mappings. `FFIEC CAT` has no successor framework, so customers using it must migrate manually.

– Lists exact retired frameworks and flags the one with no successor

Plerion's compliance frameworks, rebuil…

THINNER COVERAGE BELOW

04 **18 frameworks promoted to latest editions** IMPROVED

56

18 frameworks were promoted to their publisher's latest edition, including `PCI DSS 4.0.1`, `NIST SP 800-53 Rev 5 Release 5.2.0`, `CSA CAIQ v4.1`, `UK NCSC CAF 4.0`, and `FedRAMP Rev 5 CR26` baselines.

— Names exact versions but no mechanism or next-step guidance

Plerion’s compliance frameworks, rebuil…

└──▷ **BREAKING ON UPGRADE**

! Compliance posture percentages will shift in both directions across all 40 rebuilt frameworks because the control-to-detection mappings were reconstructed rather than patched.

! 23 retired framework editions (including PCI DSS 4.0, PCI DSS 3.2.1, NIST CSF v1.1, ISO/IEC 27001:2013, CIS AWS Foundations Benchmark v4.0.1, and FFIEC CAT) are removed from the framework list; FFIEC CAT has no successor framework.

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

Minimus

Feedback ⓘ 1 RELEASE · 2026-08-16 NOTES ↗

> Minimus's August 16, 2026 release adds package-level advisory filtering, a per-CVE breakdown of affected packages, and expanded visibility into action rule execution via status indicators and Activity Log integration.

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

01 **Action rule status tracking and Activity Log integration**

IMPROVED 72

Action rules now display a status indicator for their most recent invocation and a running count of how many times they have triggered. Every action rule invocation, success or failure, is written to the Activity Log, with a new Open Action button on each log entry to jump directly to the related action rule.

— Names UI elements and log behavior with clear navigation August 16, 2026

02 **Affected package breakdown per CVE in vulnerabilities tab**

NEW 60

Adds a breakdown of affected packages within each origin package per CVE/GHSA in the image vulnerabilities tab summary, with a link to a pre-filtered advisories view.

— Names the tab and linked view but no exact path August 16, 2026

THINNER COVERAGE BELOW

03 **Package column and filtering in Advisories table** NEW

57

Adds a Package column alongside the existing Origin Package column in the Advisories table, enabling filtering by both the origin package and the affected package.

— Names both columns but no filter mechanics detail August 16, 2026

04 **Detected column removed from Advisories table** BREAKING

45

The Detected column has been removed from the Advisories table and is now only accessible in the detailed dialog.

— Clear before/after but minimal follow-up guidance August 16, 2026

└──▷ BREAKING ON UPGRADE

! The `Detected` column has been removed from the Advisories table and is now only accessible in the detailed dialog.

WAS THIS USEFUL? 👍 👎

Chainguard

Feedback ⓘ 1 RELEASE · 2026-08-10 NOTES ↗

Chainguard provides container image security and supply chain management solutions, offering hardened, minimal Linux images and vulnerability scanning.

> Chainguard published its full public API surface (260 endpoints across 59 areas), added an AWS Security Hub Extended integration for Libraries findings, introduced a beta malware-visibility tab in the Console, added PKCE support for custom OIDC identity providers, and shipped 23 new container images.

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

01 **AWS Security Hub Extended integration for Libraries** NEW 70

Chainguard Libraries findings are now distributed through AWS Security Hub Extended, with findings normalized to the Open Cybersecurity Schema Framework (OCSF) and AWS Enterprise Support (Level 1) available for eligible customers; customers subscribe and pay through their existing AWS account from the Security Hub console.

— Explains mechanism and eligibility; subscribe path named but no exact steps

Week of 2026-08-10

02 **Malware tab in Console Libraries section** NEW 70

A new Malware tab (beta) in the Libraries section of the Console shows malicious and suspicious packages blocked before reaching an environment, with a weekly chart covering Python and JavaScript ecosystems and a per-package search that explains why a package was flagged. It is enabled by default for all Libraries-entitled organizations.

Review malware and greyware blocked across your Libraries-entitled organization directly in the Console.

> 📍 In the Console, go to Libraries › Malware tab to view the weekly blocked-package chart and search for any flagged package to see the reason it was marked unsafe.

— Exact Console navigation and behavior given, no command-line surface Week of 2026-08-10

03 **Public API launch across 59 resource areas** NEW 65

Chainguard now publishes a public API spanning 260 endpoints across 59 areas, documented at `https://edu.chainguard.dev/api.json`. The largest areas are Registry (33 endpoints, create/read/update/delete), Registryentitlements (11), Identityprovidersservice (9), Groupsservice (8), Identityproviders (8), Advisories (7), Groups (7) and Identitiesservice (7), plus 51 further areas: Reposervice , Accountassociationsservice , Policies , Rolebindingsservice ,

Awsmarketplacesubscriptions , Actionsauthorization , Externalgrouprolemappings , Externalgrouprolemappingsservice , Groupaccountassociations , Iamidentities , Rolebindings , Rolesservice , Argosdocuments , Argososv , Auth , Bindings , Groupinvitesservice , Librariesresolutioncache , Librarypolicies , Librarypolicybindings , Roles , Subscriptionsservice , Tagsservice , Vulnerabilities , Artifacts , Artifactsservice , Groupinvites , Librariesentitlements , Overrides , Securityadvisory , Securityadvisoryservice , Securitytokenservice , Skillsentitlements , Subscriptions , Apk , Advisoriesservice , Apko , Argosvulns , Charts , Imagesservice , Npmpackages , Pingservice , Terms , Termsservice , Actions , Decisions , Eventidentities , Imagematcher , Librarypolicyblockevents , Malware , Packagesentitlements .

— Names every area and endpoint count but no auth or request detail v1

04 **PKCE support for custom OIDC identity providers** NEW

65

Adds Proof Key for Code Exchange (PKCE) support for OAuth token exchange with custom OIDC identity providers, aligned with OAuth 2.1, configurable via `chainctl` or the Chainguard API, and usable alongside an existing client secret or as a secret-free public client.

— Names chainctl/API config path but no exact flag or endpoint Week of 2026-08-10

THINNER COVERAGE BELOW

05 **23 new container images** NEW

50

Adds 23 new container images: `prometheus-stackdriver-exporter` (+FIPS), `crossplane-azure-keyvault` , `crossplane-azure-kusto` , `influxdb-fips` , `moodle-iamguarded` , `pypiserver-fips` , `kubevirt-cdi-cloner` (+FIPS), `yopass` , `acm-controller` (+FIPS), `gremlin-server` , `rollouts-plugin-trafficrouter-gatewayapi` (+FIPS), `claude` , `codex` , `cruise-control` (+FIPS), `dotstatsuite-supercore` , `opencode` , and `zalando-pgbouncer` (+FIPS).

— All image names listed but no pull command or registry path given Week of 2026-08-10

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Detection Engineering

Tenzir

Feedback ⓘ 1 RELEASE · 2026-08-17 CHANGELOG ↗

Tenzir is a security data platform that ingests, transforms, and analyzes security telemetry and threat intelligence data.

> Tenzir expanded detection capabilities with Sigma 2.1 and YARA-X support, and introduced native time-series analytics for beacon detection.

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

01 **Sigma 2.1 and YARA-X detection support** NEW 30

Tenzir Node v6.11.0 adds detection support for `Sigma 2.1` and `YARA-X`, expanding the rule formats the platform can evaluate against ingested telemetry.

— Names two formats but no mechanism or usage detail. changelog-20260817-c1bc7041

02 **Native time-series analytics for beacon detection** NEW 25

Tenzir Node v6.10.0 introduces native time-series analytics aimed at beacon detection use cases.

— States purpose only, no mechanism or configuration shown. changelog-20260817-c1bc7041

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Sophos Protection for Linux

Feedback ⓘ

4 RELEASES · SEEN 2026-08-17 NOTES ↗

Sophos Protection for Linux is an endpoint security tool that provides threat detection, malware prevention, and vulnerability management for Linux systems.

> Sophos Protection for Linux added core threat-protection capabilities — on-access scanning with automatic quarantine and network device isolation — alongside ARM64 server support, more flexible installers, path-based allow-listing, and Helm chart output configuration for the Linux Sensor.

└──▷ **WHAT SHIPPED · 7 FEATURES** most completely described first ? what's the number?

01 **Allow-list applications by filename or path** NEW 75

Adds allow-list-by-path support for Linux, letting users permit applications by filename or path, configurable from event details or at `General Settings > Allowed Applications` in Sophos Central.

Allow a specific application by path to suppress false-positive detections on a Linux endpoint.

> 📍 In Sophos Central, go to General Settings › Allowed Applications and add the application by filename or path.

— Exact UI navigation path plus a usage example Version 2024.1

02 **On-access scanning and automatic malware quarantine** NEW 70

Adds on-access file scanning for the Sophos Linux Agent, configurable via server threat protection policies in Sophos Central and off by default. Also introduces malware quarantine covering both on-access and on-demand scanning, automatically isolating files on signature match.

— Names policy location and default state but no exact config key Version 2023.1

03 **Device Isolation for Linux endpoints** NEW 65

Adds Device Isolation for Linux: isolate a Linux endpoint from the network via Sophos Central while retaining management connectivity, using the existing isolate, remove-from-isolation, and exclusion controls.

— Describes mechanism and controls but only points to Sophos Central UI Version 2024.1

THINNER COVERAGE BELOW

04 **Helm chart alert and event output configuration** IMPROVED

55

Helm chart `1.0.4` adds configuration of alert and event outputs, allowing operators to control where detections from the Sophos Linux Sensor are routed.

— Names the chart version and capability but no config keys shown Version 5.15.1New

05 **ARM64 server support for SPL Agent** NEW

45

Supports installing the SPL Agent on ARM64-based Linux servers, enabling Linux Runtime Detections on ARM64 hardware.

— States platform support but no install steps or requirements Version 2023.4

06 **Installer options: custom path and pre-install checks** NEW

45

Adds an installer option to designate a custom install location for the SPL Agent, and a separate installer option to run pre-installation checks without installing the SPL Agent, enabling environment verification and troubleshooting.

— Names two installer options but not their exact flags Version 2023.4

07 **Linux Runtime Detections service in Security Health** BREAKING

40

Includes the Sophos Linux Runtime Detections service in the Security Health view in Sophos Central, updating the health state reported for Linux devices; upgrading may change the reported security health state for Linux devices.

— Notes the behavior change but no remediation steps given Version 2024.1

└──▷ **BREAKING ON UPGRADE**

! Adding the Sophos Linux Runtime Detections service to Security Health may change the reported security health state for Linux devices in Sophos Central after upgrading.

WAS THIS USEFUL?  

Sophos Mobile (on-premises)

Feedback ⓘ

1 RELEASE · SEEN 2026-08-17 NOTES ↗

Sophos Mobile on-premises is an enterprise mobile device management solution for securing and managing iOS, Android, and other mobile devices within organizations.

> Sophos Mobile 9.7 adds Apple User Enrollment for BYOD iOS devices, expands iOS Web Content Filter and Per App VPN policies, and drops support for a range of legacy OS versions while tightening Android Enterprise enrollment requirements.

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

01 **Dropped OS support and Android Enterprise enrollment enforcement**

75

BREAKING

Support for Android 5, Android 6, iOS 11, macOS 10.13, Windows 10 Enterprise version 1709, Windows 10 Education version 1709, Windows 10 Pro version 1903, and Windows 10 Home version 1903 is dropped in this version. Additionally, Android 10 or later devices must now be enrolled using Android Enterprise; enrollment via the legacy Device administrator mode will fail for these devices.

— Lists exact dropped versions and clear enrollment migration path Sophos Mobile 9.7

02 **Apple User Enrollment management mode** NEW

60

Adds Apple User Enrollment as a new management mode for user-owned iPhones and iPads, isolating work apps and data in a separate volume from personal data.

— Names the mode and isolation mechanism but no config steps Sophos Mobile 9.7

THINNER COVERAGE BELOW

03 **Kiosk mode notification toggle** NEW

45

Adds a new Show notifications setting to the Android Enterprise Kiosk mode policy, enabling notifications to be toggled on or off for kiosk devices.

— Names exact policy setting, clear toggle to apply Sophos Mobile 9.7

04 **Per App VPN domain-triggered connections** IMPROVED

45

Adds additional domain settings to the iOS Per App VPN policy to establish VPN connections when domains are opened in Calendar, Contacts, or Mail.

— Explains trigger mechanism but no field names given Sophos Mobile 9.7

05 **Migration token requirement removed** IMPROVED 40

Removes the migration token requirement when migrating from Sophos Mobile on-premises to Sophos Central.

— Clear before/after but no procedural detail Sophos Mobile 9.7

06 **iOS Web Content Filter third-party integration settings**

IMPROVED 25

Adds additional settings to the iOS Web Content Filter policy for integrating third-party web filtering services.

— No specific settings or vendors named Sophos Mobile 9.7

└──▷ **BREAKING ON UPGRADE**

! Support for Android 5, Android 6, iOS 11, macOS 10.13, Windows 10 Enterprise version 1709, Windows 10 Education version 1709, Windows 10 Pro version 1903, and Windows 10 Home version 1903 is dropped in this version.

! Android 10 or later devices must now be enrolled using Android Enterprise; enrollment via the legacy Device administrator mode will fail for these devices.

WAS THIS USEFUL? 👍 👎

Sophos Intercept X for Mobile

Feedback ⓘ

1 RELEASE · SEEN 2026-08-17 NOTES ↗

Sophos Intercept X for Mobile is an endpoint protection platform that detects and prevents malware, ransomware, and threats on iOS and Android devices.

> Sophos Intercept X for Mobile 9.7.7 extends its User Activity Verification API to support URL-based actions.

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

01 **URL support in User Activity Verification API** IMPROVED

50

The Sophos User Activity Verification API now supports URLs, enabling requests that open a web page or initiate a phone call when a user selects an option.

— Names the API and new behavior but no endpoint or field details Version 9.7.7

WAS THIS USEFUL? 👍 👎

Sophos Central

Feedback ⓘ

2 RELEASES · SEEN 2026-07-20 → 2026-08-17 NOTES ↗

Sophos Central is a cloud-based unified security management platform for protecting endpoints, servers, networks, and email across organizations.

> Sophos Central's latest updates center on identity threat detection expansion with ML-derived Identity Risk Scores and new regions, alongside a new Network Map for visualizing Sophos network topology and a lightweight Protected Browser extension for Chrome and Edge.

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

01 **Identity Risk Scores in Sophos ITDR** NEW 58

Sophos ITDR now surfaces a single ML-derived Identity Risk Score combining incident likelihood and compromise impact for each identity, which updates dynamically as findings and account details change.

— Mechanism described but no UI path or API given Latest news

02 **Network Map topology visualization** NEW 58

A new Network Map provides a visual representation of Sophos network topology, showing relationships and connections between all Sophos firewalls, switches, and AP6 access points in a Central account, with search capabilities.

— Names devices and search feature, no exact navigation path July 20, 2026

03 **Workspace Protection Protected Browser extension** NEW 58

A new Workspace Protection: Protected Browser extension for Chrome and Edge lets administrators apply security policies and monitor user activity without requiring migration to the full Sophos Protected Browser.

— Names browsers and product relationship, no install steps given July 20, 2026

04 **Live Discover queries for AP6 access points** IMPROVED 55

Live Discover queries now support AP6 Series access points, enabling on-demand querying of wireless data stored in the Sophos data lake.

— Names data source and device series, no sample query given July 20, 2026

05 **Generative AI category in DNS Protection filtering** NEW 48

DNS Protection filtering policies gain a new Generative AI category, giving visibility into AI service usage on networks and enabling policy-based control over it.

— Names the exact category and policy area, no config detail Latest news

06 **Sophos AI Defense Early Access Program** NEW 43

Sophos AI Defense EAP launches for Sophos EDR, XDR, and MDR customers on Sophos Fusion, enabling monitoring, control, and security of AI usage across an environment.

— Names eligible products and platform but no enrollment steps Latest news

07 **Partner bulk license add-on selection** IMPROVED 42

Partners can now explicitly select individual add-ons and products when applying bulk license changes to multiple monthly-usage customers simultaneously, rather than affecting all licenses at once.

— Explains the workflow change but no exact console path Latest news

08 **Sophos ITDR regional expansion** IMPROVED 33

Sophos ITDR is now available to tenants provisioned in Canada, Australia, Japan, India, and Brazil.

— Names regions but no further mechanism or action Latest news

WAS THIS USEFUL? 👍 👎

◆ SIEM

Sumo Logic

Feedback ⓘ 1 RELEASE · 2026-08-17 BLOG ↗

Sumo Logic is a cloud-based monitoring and analytics platform for logs, metrics, and security data.

> Sumo Logic introduced AI Parse Assist, a search feature that auto-generates parse statements and field names from highlighted log text to speed up query building.

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

01 **AI Parse Assist in Search** NEW 45

A new AI Parse Assist feature automatically generates a parse statement and field names from any text highlighted in a log message, accelerating query building for complex or unfamiliar log formats.

— Describes behavior but no exact UI path or syntax.

AI Parse Assist (Search) (2026-08-17)

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Intruder

Feedback ⓘ 1 RELEASE · 2026-08-17 BLOG ↗

Intruder is a cloud-based vulnerability scanner that automatically discovers and tests systems for security weaknesses.

> Intruder introduced a dark theme option that users can toggle in Settings, with the preference automatically saved across sessions.

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

01 **Dark theme toggle in Settings** NEW 40

Adds a dark/light theme toggle in Settings, with the chosen preference persisted automatically across sessions and applied consistently across dashboards, search, and widgets.

— Names UI location and persistence behaviour, but no config/API detail.

Dark theme is here! (2026-08-17)

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

Cloudmersive

Feedback ⓘ 1 RELEASE · 2026-08-16 BLOG ↗

Cloudmersive is an API platform providing cloud-based document processing, image manipulation, and data conversion services for developers.

> Cloudmersive's Private Cloud Convert API v7-7-1 adds a customizable PDF Creator setting.

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

01 **Customizable PDF Creator setting** NEW 25

The Convert API now supports a customizable PDF Creator setting, allowing the creator metadata field on generated PDFs to be configured.

— No field name, endpoint or config detail given, just a brief description.

Cloudmersive Private Cloud Convert API …

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

DNSFilter

Feedback ⓘ 1 RELEASE · 2026-08-17 CHANGELOG ↗

DNSFilter is a security tool that filters DNS queries to block malicious domains, ads, and unwanted content at the network level.

> DNSFilter shipped DNS PreCheck v2 to close a policy-enforcement gap on DNS-hijacking networks, alongside a reorganized policy/schedule dropdown.

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

01 **DNS PreCheck v2 for DNS-hijacking networks** NEW 60

DNS PreCheck v2 maintains policy enforcement on networks that hijack or redirect DNS traffic, closing a gap where certain network conditions could previously allow content through that should have been blocked. The agent tray updates to display `DNS PreCheck v2` when the feature is active.

— Explains the gap closed and the tray indicator, but no config detail.

changelog-20260817-70bf97bd

02 **Organization grouping in policy/schedule dropdown** IMPROVED 60

The Policy/Schedule dropdown now groups an organization's own policies under an `Organization` header, with sections ordered Organization, Global, then Scheduled. This applies across Sites, Roaming Clients, Relays, Subnets, Users, and Collections.

— Names exact UI areas and ordering; navigable but no deeper mechanism.

changelog-20260817-70bf97bd

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

Auth0

Feedback ⓘ 1 RELEASE · 2026-08-17 CHANGELOG ↗

Auth0 is a cloud-based identity and access management platform providing authentication, authorization, and user management solutions for applications.

> Auth0 GA'd a unified Flexible Password Policy for database connections and extended Custom Prompts data capture to Social and Enterprise connections.

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

01 Flexible Password Policy for database connections

BREAKING

95

Adds an `options.password_options` object to database connections, replacing the legacy fields `passwordPolicy`, `password_complexity_options`, `password_history`, `password_no_personal_info`, and `password_dictionary` with granular controls for password composition, history, dictionary blocking (10,000- or 100,000-word lists plus custom entries), and profile-data blocking. It's configurable via the Auth0 Dashboard under Authentication > Database > [your connection] > Authentication Methods > Password, or through the Management API. New database connections created from July 2026 onward default to Flexible Password Policy — minimum password length of 15, no required character types, no legacy fields — regardless of whether the connection is created via Dashboard, Management API, Deploy CLI, Terraform, or an Auth0 SDK. As a breaking change, `PATCH /api/v2/connections/{id}` now returns `400 invalid_body` if the request body includes both `password_options` and any legacy password field, so automations that read-then-write connections with legacy fields appended must be updated to send only `password_options`.

— Names exact config object, legacy fields, endpoint and error code.

changelog-20260817-ff823779

THINNER COVERAGE BELOW

02 Custom Prompts extended to Social and Enterprise connections

IMPROVED

58

Custom Prompts — the custom signup/login fields and consent checkboxes configured in Universal Login — now capture data on Social and Enterprise connections in addition to database and passwordless connections, with no configuration changes required. Existing setups are reviewable under Branding → Universal Login → Enhance screens with partials, or via the Management API.

— Names UI path and API but no new mechanism detail. changelog-20260817-ff823779

└──▷ **ALSO FROM THESE RELEASES**

.
.
.
.

└──▷ **BREAKING ON UPGRADE**

! `PATCH /api/v2/connections/{id}` returns `400 invalid_body` if the request body includes both `password_options` and legacy password fields (`passwordPolicy` , `password_complexity_options` , `password_history` , `password_no_personal_info` , `password_dictionary`). Automations that read a connection and write it back with legacy fields appended must be updated to send only `password_options` .

! New database connections created from July 2026 default to Flexible Password Policy (minimum length 15, no required character types) rather than legacy password policy defaults. Automations that create connections without specifying a password configuration will receive these new defaults instead of the previous legacy behavior.

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

CISO Assistant

Feedback ⓘ 1 RELEASE · 2026-08-17 NOTES ↗

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 150+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

> CISO Assistant v3.21.1 adds HTTP transport to its aggregated MCP architecture, extends framework coverage with CyFun2025 and ISO27001 mapping, and ships smaller improvements across TPRM, evidence filtering, assessments and approvals.

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

01 **HTTP transport for aggregated MCP** NEW 55

CISO Assistant's aggregated MCP (Model Context Protocol) architecture now supports `http` transport, expanding AI coverage and reducing token usage on context in agentic workflows.

– names the transport but gives no config or usage steps v3.21.1

02 **Library validation tool check_library_v2.py** NEW 50

Adds `check_library_v2.py` tool for library validation.

– named runnable script but no usage instructions given v3.21.1

03 **CyFun2025 and ISO27001 framework mapping** NEW 45

Adds CyFun2025 and ISO27001 framework mapping to the library (`lib`), extending automatic control mapping coverage.

– names frameworks but not mapping mechanism v3.21.1

04 **Unassigned evidence filter** NEW 45

Adds an assignee null option to the evidences filters list, allowing filtering for unassigned evidence items.

– clear filter option with obvious UI location v3.21.1

05 **Audit link modes in TPRM wizard** NEW 40

Adds audit link mode options in the TPRM data wizard for entity configuration, giving different linking modes when setting up third-party audits.

– no detail on which link modes exist v3.21.1

06 **Author columns in assessments views** NEW 30

Adds optional authors columns to assessments views.

— bare description with no further detail v3.21.1

07 **Conditional incidents in analytics** IMPROVED 20

Conditionally enables incidents in analytics based on configuration.

— no detail on the triggering configuration v3.21.1

08 **Streamlined approval management interface** IMPROVED 20

Delivers a streamlined interface for approval management.

— no specifics on what changed in the UI v3.21.1

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Daytona

Feedback ⓘ 1 RELEASE · SEEN 2026-08-17 NOTES ↗

Daytona is a development environment platform that enables standardized, reproducible coding spaces for teams and AI agents.

> Daytona shipped two SDK/API improvements this window: a lifecycle-aware filter for querying sandboxes by destruction time, and structured, typed error responses in the SDK.

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

01 **autoDestroyAt filter on sandbox list endpoint** NEW

60

The sandbox list endpoint now supports an `autoDestroyAt` range filter, enabling lifecycle-aware queries that scope results by scheduled destruction time.

— Names the filter but not exact endpoint path or method snapshot-20260817

THINNER COVERAGE BELOW

02 **Typed SDK error codes** NEW

50

The SDK now returns structured error responses with typed error codes, giving programmatic access to failure reasons instead of requiring raw HTTP status parsing.

— Describes mechanism but no code example or field names snapshot-20260817

WAS THIS USEFUL? 👍 👎

AGENT

◆ AI Agent Frameworks

Hermes

Feedback ⓘ 1 RELEASE · 2026-08-16 NOTES ↗ CODE ↗

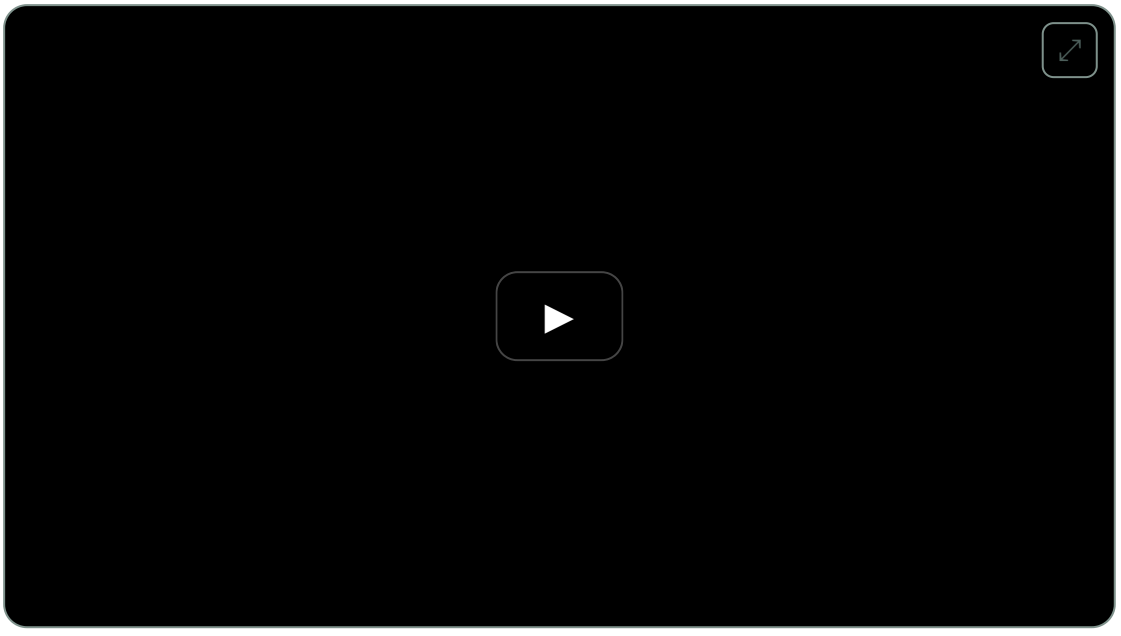
The agent that grows with you

> Hermes shipped a wide config and integration expansion this window: personal `AGENTS.override.md` files, several MCP protocol hardening and metadata changes, a new lean compaction mode and subagent delegation routing, expanded CUA driver health/permissions tooling, and a key_cmd credential-sourcing mechanism with matching plugin SDK exports.

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

01 **tail_mode compaction control** NEW 90

Adds `tail_mode` config key with `legacy` (0.20× window verbatim tail) and `lean` (clamped 2.5% tail, 10K–25K tokens, with digests, anchor index, and `session_search` recovery pointers) modes; `lean` yields roughly 3× fewer retained tokens after compaction.



— Exact config key, both modes, and quantified token reduction. product docs

02 **CUA driver health checks, permissions, and browser authorization**

NEW 90

Adds `doctor [--include CHECK] [--skip CHECK] [--json]` to run cua-driver's health report, `permissions status [--json]` and `permissions grant` to report and request macOS Accessibility and Screen Recording grants, and `hermes computer-use status` to surface when cua-driver repair is required. Supports the

`HERMES_CUA_DRIVER_CMD` environment variable to pin a custom cua-driver binary that Hermes never replaces during auto-repair, and `--capability-manifest` / `--approve-capability-manifest` flags in bounded mode; `cua-driver skills install` now auto-detects Hermes and links Cua's skill pack into the Hermes skills directory. A user-facing authorization flow was also added for cua-driver browser attachment in computer-use mode.

— Enumerates every named command, flag, and env var, all runnable. v2026.8.16

---

03 **key_cmd credential sourcing for providers** NEW 90

Adds `key_cmd` credential source to provider config, letting operators specify a shell command that prints a short-lived token instead of storing a static key — output can be a bare token or JSON with `access_token` and optional `expires_in` fields; the token is cached until near expiry.

Use a short-lived SSO token for an enterprise gateway without storing a static key in .env — the command runs once per token lifetime and the fresh bearer is used on every request.

yaml

```yaml
providers:
  my-gateway:
    base_url: https://gateway.internal.example.com/v1
    api_mode: chat_completions
    key_cmd: my-auth-cli print-token --profile prod
```

— Exact config key, field names, and a runnable YAML example. v2026.8.16

---

04 **delegation.* subagent model routing** NEW 75

Adds a `delegation.*` config section for subagent model routing: the `entry` key controls which provider, model, and credentials subagents inherit, with `inherit` meaning 'use the parent agent's settings'; settings persist to `delegation.*` rather than `auxiliary.*` because subagents are full child agents.

— Names exact config keys and their semantics. product docs

---

05 **CLI multiline input and scrollback config keys** NEW 75

Adds `cli_multiline_shortcuts` config key to enable Ctrl+J, `\` + Enter, and Shift+Enter as newline-insert shortcuts in the CLI (false restores legacy Ctrl+J submit behavior), and `cli_rebuild_scrollback_on_redraw` to issue a CSI 3J wipe of terminal scrollback on `/redraw`, Ctrl+L, or resize recovery — useful when a terminal or tmux stack stamps stale prompt chrome into scrollback on maximize/restore.

— Both exact config keys and their triggers named. product docs

---

06 **Plugin SDK exports for capability config panels** NEW

75

Exports `McpTab`, `ToolsetConfigPanel`, and `HermesGateway` types from `@hermes/plugin-sdk`, plus a host.getGateway() method returning the live `$gateway` instance, so desktop plugins can render full credential, OAuth, and MCP server configuration panels matching Settings → Capabilities.

— Names exact exported types and method for plugin authors. v2026.8.16

07 **Personal AGENTS.override.md context files** NEW 70

Adds support for an `AGENTS.override.md` file placed next to a committed `AGENTS.md`; when present it is loaded instead of the tracked file, intended to be gitignored so individuals can keep personal agent instructions without modifying the shared file.

Keep personal agent instructions that differ from the team's committed `AGENTS.md` without touching the tracked file.

```
$ echo 'Always respond in Spanish.' > AGENTS.override.md
echo 'AGENTS.override.md' >> .gitignore
```

— Names exact file and gitignore workflow with a runnable example. product docs

08 **UTF-16 file auto-transcoding for display and edits** IMPROVED

70

UTF-16 files (detected via BOM or byte-pattern heuristic, either endianness — covering Windows Notepad files and PowerShell redirects) are transcoded to UTF-8 for display instead of being refused as binary, with a hint disclosing the conversion; edits via `write_file` re-encode as UTF-8, while files over 10 MB and genuinely binary files still receive the binary-file refusal.

— Names detection method, size limit, and the write_file behavior. product docs

09 **MCP server suggestion pills in composer** NEW 65

MCP server manifests can now include a `suggest` block with `keywords` and `hosts` lists that trigger one-click Add <server> pills in the Desktop app composer when a matching word or hostname appears in a draft.

— Names the manifest field and trigger fields but no runnable command. product docs

10 **MCP `_meta` field passthrough** NEW 65

Surfaces vendor `_meta` mappings (e.g. `com.example/handoff`) from MCP tool results to the model, while dropping protocol-reserved keys under

`modelcontextprotocol` and `mcp` prefixes (e.g. `modelcontextprotocol.io/...`, `tools.mcp.com/...`); omits `_meta` entirely when no model-facing keys remain.

— Exact key patterns named but passive, no user action. product docs

11 **Unicode TAG character stripping from MCP results** NEW

60

Strips invisible Unicode TAG characters in the U+E0000–U+E007F range from MCP tool results, resource content, and tool descriptions to block prompt-injection smuggling, while preserving legitimate emoji tag sequences such as regional flags.

— Precise range and rationale given but it's an automatic, non-actionable fix. product docs

12 **Interactive session picker with search and resume** NEW

60

Adds an interactive session picker with search, resume, lifecycle status tags (`done`, `intr`, `err`, `empty`), message counts, and delete-with-confirmation.

— Named status tags but reached via UI, not a command. product docs

THINNER COVERAGE BELOW

13 **GitHub routed through github-auth skill instead of MCP catalog**

IMPROVED

50

GitHub is intentionally excluded from the MCP hosted catalog; Desktop instead offers the `github-auth` skill when `gh` is not signed in, routing through bundled `github/*` skills that drive the `gh` CLI.

— Names the skill and CLI dependency but limited mechanism detail. product docs

14 **Signal-kill exit annotations for terminal commands** IMPROVED

50

Terminal commands killed by a signal now carry a human-readable annotation in the result — e.g. exit code `-9` / `137` becomes 'terminated by signal 9: SIGKILL — often the kernel OOM killer on memory exhaustion, or an explicit kill -9'; segfaults, aborts, SIGTERM, broken pipes, and CPU/file-size limit signals are labeled the same way.

— Concrete examples of exit codes but no user action required. product docs

15 **Multi-source agent support in desktop app** NEW

35

Adds multi-source agent support to the desktop app — sockets, roster, SDK, and fan-out updates are now handled end-to-end.

— Names the sources but no mechanism or usage detail. v2026.8.16

16 **Desktop turn observability improvements** IMPROVED 35

Shows per-turn wall-clock duration in the desktop transcript and adds INFO log records for 'prompt accepted / turn finished' on the Desktop/TUI turn path.

— Thin logging additions with no configuration surface. v2026.8.16

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ Agentic Infrastructure

Ollama

Feedback ⓘ 1 RELEASE · 2026-08-15 NOTES ↗ CODE ↗

Get up and running with Kimi-K2.6, GLM-5.2, MiniMax, DeepSeek, gpt-oss, Qwen, Gemma and other models.

> Ollama v0.32.14 adds WebP image support for vision models and fixes a crash when Qwen receives system messages mid-conversation.

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

01 **WebP image transcoding for vision models** NEW 53

Ollama automatically transcodes WebP image payloads to PNG before forwarding them to llama-server, extending vision model support beyond the existing JPG and PNG formats.

— Explains mechanism and formats but no config or flag given v0.32.14

02 **Non-leading system messages in Qwen renderer** IMPROVED 53

The Qwen renderer now passes non-leading system messages through the raw ChatML path instead of returning an HTTP 500, allowing coding clients that inject runtime system prompts mid-conversation to function correctly.

— Names the bug, error code, and mechanism, but no direct user action v0.32.14

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

AI-Infra-Guard

Feedback ⓘ 1 RELEASE · 2026-08-17 NOTES ↗

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 v4.5.2 adds passive fingerprinting for popular vector databases, kicks off a new jailbreak research track, and ships a breaking refactor of its agent red-team mutation engine.

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

01 **Mutation engine refactor merges workflow-attack into mutation-attack**

65

BREAKING

Upgrades the `aig-agent-redteam` skill to v5.0.0 with a refactored mutation engine that merges `workflow-attack` into `mutation-attack` for consolidated adversarial testing. This is a breaking change: any automation or config referencing `workflow-attack` as a separate attack mode will need to be updated.

— Names skill, version and exact attack modes affected v4.5.2

THINNER COVERAGE BELOW

02 **GET-only fingerprints for Qdrant, Chroma, Weaviate** NEW

43

Adds GET-only fingerprints for Qdrant, Chroma, and Weaviate to the fingerprint library, enabling passive identification of these vector databases.

— Names three products but no scan command shown v4.5.2

03 **New AIG detection rules** NEW

15

Adds new AIG detection rules dated 2026-07-31.

— No description of rule content or coverage v4.5.2

04 **SkillJack research project** NEW

10

Introduces the SkillJack research project, expanding the platform's AI security research surface.

— Bare mention with no detail on scope or use v4.5.2

└──▷ **BREAKING ON UPGRADE**

! The `aig-agent-redteam` skill's `workflow-attack` has been merged into `mutation-attack`; any automation or config referencing `workflow-attack` as a separate attack mode will need to be updated.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · August 17, 2026

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

▷ **Subscribe** Feedback on this issue