THE CYBER TOOLCHAIN

NO. 105

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 12, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 66 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 18 tools

▾ // THE BRIEF HIDE

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

IDENTIFY

See the non-human identities Entra created while nobody was looking

vim ? help

Agent and service identities get provisioned by developers and platform teams faster than any directory review catches them, and they rarely have an owner. Sophos Central now enumerates AI agents and non-human identities created via Microsoft Entra; Sophos Switch's Network Map adds persistent layouts and SVG export, so the topology you built survives a reload and can go into a report.

Sophos Central · Sophos Switch

PROTECT

Catch the security bugs that live in the design, not the line

SAST matches patterns in a single file and SCA matches package names, so a missing authorization check between two correct-looking functions passes both. Endor Labs' multi-agent review reads the pull request for architectural risk; Snyk Code's rule refresh spans nine languages with better template and serverless analysis, where context-free scanners usually go blind.

Endor Labs · Snyk Code

GOVERN

Revoke or exempt a shared CI token once, not once per org

Classic PATs with broad scope get shared across repos and orgs, and auditing them has meant walking each org's settings page separately. StepSecurity's tenant-wide exemptions put that decision in one place; Cloudsmith's Rego validation endpoint lets you test a policy before it starts blocking real package pulls.

StepSecurity · Cloudsmith

OFFENSIVE SECURITY

◆ AI-Powered Offensive Security

PurpleAILAB Decepticon

Feedback ⓘ v1.4.0 NOTES ↗

RANK

Autonomous Hacking Agent for Red Team

> Decepticon v1.4.0 introduces explicit Plan, Red, and Blue operating modes with safety checks, expands its planning interview to cover all nine planning documents, and extends model support with production LiteLLM routes and selectable local Ollama models.

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

01 Plan, Red, and Blue run modes NEW

90

Adds Plan, Red, and Blue run modes switchable via the CLI `/mode` command (e.g. `/mode Plan`, `/mode Red`, `/mode Blue`), the OSS launcher, and the web live view. Red mode requires one confirmed target and an authorization reference and rechecks RoE approval on start; Blue mode checks both sensor and monitor health before engaging the resident defensive agent.

Switch the running session into Red mode to begin an engagement directly from a confirmed target without going through the full Plan interview.

```
$ /mode Red
```

Switch into Plan mode to invoke Soundwave's eight-document planning interview before committing to a Red engagement.

```
$ /mode Plan
```

Switch into Blue mode to bring the resident defensive agent into the explicit mode flow, triggering sensor and monitor health checks alongside the engagement.

```
$ /mode Blue
```

— Names exact commands, modes, and their safety checks v1.4.0

THINNER COVERAGE BELOW

02 Expanded Plan document views IMPROVED

45

Adds five additional Plan document views, making all nine planning documents visible in the Plan view (part of Soundwave's planning interview).

— Gives a count but no concrete key or path to the documents v1.4.0

03 **LiteLLM routing and Ollama model selection** IMPROVED

45

Brings current production LiteLLM model routes into the OSS agents and CLI, and adds selectable local Ollama model IDs.

— Names LiteLLM and Ollama but no command to select a model v1.4.0

04 **Health surface model count and service details** IMPROVED

35

Adds complete LiteLLM model count and concise service health details to the health surface.

— Thin description with no path or endpoint for the health surface v1.4.0

05 **Engagement-scoped report tool calls** NEW

15

Adds engagement-scoped report tool calls.

— One-line mention with no mechanism or usage detail v1.4.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ Software Supply Chain Security

Cloudsmith

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗

RANK

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

> Cloudsmith shipped a Rego policy validation API endpoint alongside several Cloudsmith CLI upgrades, including a workspace-scoping flag, built-in self-update, a Terraform credential helper, and more resilient SSO sessions.

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

01 **CLI self-update capability** NEW 65

Adds a built-in self-update capability to the Cloudsmith CLI (v1.27.0+) so the CLI can upgrade itself without external tooling.

Upgrade the Cloudsmith CLI to the latest version using its built-in self-update, then switch to a specific workspace context.

```
$ cloudsmith update
cloudsmith --workspace <workspace-slug> <subcommand>
```

— Runnable `cloudsmith update` command and version gate given.

changelog-20261012-ded21a52

02 **Rego policy validate endpoint** NEW 60

Adds a `validate` API endpoint that returns syntax and type errors in Rego policy logic without creating or updating anything, enabling pre-submission policy checks.

— Endpoint name given but no HTTP method or path. changelog-20261012-ded21a52

03 **--workspace option in CLI** NEW 60

Adds a `--workspace` option to the Cloudsmith CLI to read workspace settings from the command line.

Upgrade the Cloudsmith CLI to the latest version using its built-in self-update, then switch to a specific workspace context.

```
$ cloudsmith update
cloudsmith --workspace <workspace-slug> <subcommand>
```

— Exact flag plus runnable example command. changelog-20261012-ded21a52

THINNER COVERAGE BELOW

04 **Terraform credential helper** NEW 45

Adds a Terraform credential helper to the Cloudsmith CLI that authenticates Terraform to Cloudsmith registries without storing a token.

— Mechanism stated but no setup command shown. changelog-20261012-ded21a52

05 **SSO session resilience in CLI** IMPROVED 35

Adds SSO session resilience to the Cloudsmith CLI, keeping single sign-on sessions alive through temporary network failures.

— Behavior described but no configuration or trigger named. changelog-20261012-ded21a52

WAS THIS USEFUL? 👍 👎

Endor Labs

Feedback ⓘ

Endor Labs and Bright Security Partner to Close the Gap Between Discovery and Remediatio

BLOG ↗ RANK

Endor Labs is an application security platform built for AI-generated and human-written code, helping teams prioritize and fix real risk across the SDLC.

> Endor Labs introduced AI Security Code Review, a multi-agent system that analyzes every pull request for architectural and design-level security risks missed by traditional SAST/SCA tools.

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

01 **AI Security Code Review for pull requests** NEW INTEGRATION NEW

83

Endor Labs launched AI Security Code Review, which deploys multiple AI agents (Developer, Architect, Security) to analyze every pull request for design flaws and architectural security changes that rule-based SAST/SCA tools miss. It detects security-impactful PR categories including API endpoint exposure, access control changes, authentication modifications, CI/CD workflow additions, cryptographic library swaps, database schema changes, dependency privilege escalation, input validation gaps, memory management changes, network security control modifications, payment processing integrations, and PII data handling, assigning each a priority level (Critical, High, Medium, Low) and surfacing findings in a dedicated Security Review section within each project. It integrates with the Endor Labs GitHub App to auto-trigger analysis on new PRs across a GitHub organization (surfacing submitter and reviewer identity), and connects to Endor Labs' policy engine and existing SCM/project management systems to automate ticket creation and routing, e.g. sending PII findings to GRC teams or infrastructure changes to DevOps.

Enable AI Security Code Review for your GitHub organization so every new PR is automatically analyzed for architectural security risks.

> 📍 In the Endor Labs console, go to your project settings and enable the Endor Labs GitHub App for your GitHub organization. Once enabled, AI Security Code Review will automatically run on all new pull requests and surface findings in the Security Review section of each project.

— Names detection categories, priority levels and integration points with a UI enablement path.

Introducing AI Security Code Review | B…

> Endor Labs and Bright Security Partner to Close the Gap Between Discovery and Remediat

BLOG ↗ LATEST STABLE

Endor Labs and Bright Security integrate reachability SAST with runtime DAST via SARIF handoff, enabling a CI gate and AI-agent-ready evidence for confirmed-exploitable findings only.

Adds a SARIF-based integration pipeline where Endor Labs' function-level reachability analysis passes a narrowed candidate list to Bright STAR for runtime exploit confirmation, replacing full-surface DAST sweeps.

Introduces Endor SAST + Bright STAR as a combined CI gate, catching reachable and runtime-confirmed exploitable code before it reaches the production branch.

Enables runtime-confirmed prioritization: findings Bright Security confirms exploitable at runtime are automatically elevated above reachable-but-unproven and unreachable findings.

Delivers machine-readable, verified evidence (call path from Endor Labs plus confirmed exploit path from Bright Security) to AI remediation agents, reducing token overhead for reachability and exploitability re-derivation.

WAS THIS USEFUL? 👍 👎

StepSecurity

Feedback ⓘ

PAT Governance: Tenant-Wide Exemptions (2026-10-12) BLOG ↗ RANK

StepSecurity is a security platform that hardens CI/CD pipelines and GitHub Actions workflows by detecting supply chain risks, enforcing secure configurations, and monitoring runtime behavior.

> StepSecurity shipped tenant-wide PAT exemptions for governing shared tokens across every org at once, and expanded Secure Registry with RubyGems and Cargo ecosystem support plus customizable block and hidden-version messages for npm.

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

01 **RubyGems support in Secure Registry** NEW 85

Pointing Bundler, the gem CLI, or an artifact repository manager at `https://registry.stepsecurity.io/ruby` evaluates every gem request against your RubyGems policy, enforcing Cooldown Period, Compromised Packages, and Custom Block List controls. Integration paths cover JFrog Artifactory, Sonatype Nexus Repository, and Direct.

— Exact registry URL and supported integration paths named

Secure Registry: RubyGems and Cargo Sup…

02 **Cargo support in Secure Registry** NEW 85

Pointing Cargo or JFrog Artifactory at the sparse index `sparse+https://registry.stepsecurity.io/rust/` evaluates every crate request against your Cargo policy, with Cooldown Period, Compromised Packages, and Custom Block List controls. Integration paths cover JFrog Artifactory and Direct, and existing `Cargo.lock` files keep working without being regenerated.

— Exact sparse-index URL and lockfile compatibility noted

Secure Registry: RubyGems and Cargo Sup…

03 **Custom block and hidden-version messages for npm** NEW 85

A new Block Message setting in npm Registry Settings lets you include up to 500 characters of custom text in the error developers see when a control blocks a request, using placeholders like `{{control}}` and `{{package}}`, and applies to every control except Cooldown Period. A separate Hidden Versions Notice setting, up to 300 characters with placeholders such as `{{count}}` and `{{package}}`, replaces the default notice shown when package versions are hidden by policy.

Tell developers how to request a package exception when a control blocks their npm install, using the package name in the message.

> 📍 In npm Registry Settings, set Block Message to: 'Package {{package}} was blocked by {{control}}. To request an exception, open a ticket at `https://security.example.com/exceptions.'`

— Names both settings, their limits and placeholders verbatim

Secure Registry: RubyGems and Cargo Sup…

---

04 **Tenant-wide exemptions in PAT Governance** NEW 70

Selecting `All Organizations` in the org selector and opening Apps & PATs > Exemptions now lets you click `Add tenant-wide exemption` to exempt a token or user across every organization in the tenant simultaneously. A unified exemptions view under `All Organizations` lists every organization's exemptions in one place, with tenant-wide ones labeled `Tenant-wide`.

Exempt a shared service account token from PAT Governance across all orgs in your tenant without touching each org individually.

> 📍 1. In the organization selector, choose `All Organizations`. 2. Navigate to Apps & PATs › Exemptions. 3. Click `Add tenant-wide exemption` and enter the token or user to exempt. 4. Confirm — the exemption now applies across every organization and appears labeled `Tenant-wide` in the unified exemptions list.

— Exact UI navigation given, no API or CLI surface

PAT Governance: Tenant-Wide Exemptions …

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

Snyk Code

Feedback ⓘ changelog · Oct 12, 2026 BLOG ↗ RANK

Snyk Code is a developer security tool that uses static analysis to find and help fix vulnerabilities in proprietary source code.

> Snyk Code's October update adds a wide set of new vulnerability detection rules spanning nine languages, deepens Java library coverage, and improves analysis of templates and serverless applications.

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

01 **New detection rules across nine languages** NEW 73

Snyk Code adds a Mass Assignment rule for Spring applications that flags request data binding directly onto a database entity; path traversal detection via S3 object keys for Go projects using AWS SDK for Go v2; SQL injection detection for Go; XML external entity injection detection for Python; deserialization, XML external entity injection, and zip slip detection for JavaScript; DOM-based cross-site scripting detection for JavaScript using Bootbox and d3; path traversal detection for C#; and path traversal detection plus a new server-side request forgery rule for Ruby.

– Names each rule and language but no flags or runnable commands 2026-10-12-6a54f94c

THINNER COVERAGE BELOW

02 **Expanded Java library coverage** IMPROVED 45

Java analysis adds or improves coverage for Spring Data MongoDB, AWS SDK for Java (DynamoDB), AWS SDK for Java 2.x (DynamoDB Enhanced Client), and Apache Commons FileUpload.

– Names libraries affected but not what changed in detection 2026-10-12-6a54f94c

03 **Deeper template and serverless application analysis** IMPROVED 25

Snyk Code analyzes template files and serverless applications more accurately and with greater depth, yielding additional findings in projects using template engines or serverless frameworks.

– Vague improvement with no named frameworks or mechanism 2026-10-12-6a54f94c

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Sophos Switch

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗

RANK

Sophos Switch is a network access switch from Sophos that provides managed, secure Layer 2 connectivity and power for devices, integrated with Sophos Central and firewalls.

> Sophos Switch's Network Map gains a second phase of improvements, adding SVG export, persistent layouts, and richer, more accurate device visibility across firewalls, switches, and access points.

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

01 **Network Map phase 2 enhancements** IMPROVED 85

The Network Map now supports export in SVG format, adds zoom, pan, and fit-to-view buttons, and no longer resets the view on device status refresh. It renders firewall connections and topology more accurately with offline firewalls clearly marked, shows switch names instead of serial numbers with model-appropriate port layouts and offline markers, identifies AP6 access points in a mesh as root or node and groups them for single-unit management, and gives managed/unmanaged devices better naming, a consolidated view, richer details, and reduced clutter. Device layouts can now be saved persistently so they no longer need rearranging on every visit, and a new collapsible flyout panel reduces visual obstruction.

Export a saved Network Map layout as an SVG file for inclusion in network documentation or change-management records.

📍 In Sophos Central, navigate to the Network Map, arrange and save your device layout, then select Export to download the map in SVG format.

— Names many concrete UI changes but lacks exact navigation menu path.

changelog-20261012-418a8152

WAS THIS USEFUL? 👍 👎

Sophos Access Points

Feedback ⓘ changelog · Oct 12, 2026

CHANGELOG ↗

I don't recognize a specific Sophos product called "Sophos Access Points" with confidence, so I can't describe it accurately.

Profile sort/search by name and a 50-profile limit in Sophos Fusion; richer Usage Insight with clickable client graphs and paginated category views.

Adds sort and search for access point profiles by name in Sophos Fusion.

Raises the maximum number of profiles in Sophos Fusion to 50, including the base profile.

Clicking a device in the Top 5 clients graph now navigates to its summary page for deeper bandwidth analysis.

Categories and details and Uncategorized traffic views now paginate across all categories, ports, and domains, and replace pie charts with bar graphs that update based on the visible list.

NEW SUPPORTED PLATFORM 6 GHz band steering configuration for AP6 420E and AP6 840E

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Plerion

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗ RANK

Plerion is a cloud security platform that continuously scans cloud infrastructure for misconfigurations, vulnerabilities, and compliance risks, helping teams detect and remediate threats.

> Plerion added 10 new AWS detection checks this window, spanning AgentCore IAM execution roles, Multi-AZ resilience gaps, deletion/termination protection, service quota usage, and Route 53 failover health.

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

01 **Multi-AZ resilience checks for EKS, OpenSearch, ASG, VPC** NEW 75

Adds four checks that flag single-Availability-Zone failure points: `PLERION-AWS-1244` (EKS managed node group uses subnets in a single Availability Zone, Low) — a single AZ outage removes every node; `PLERION-AWS-1245` (OpenSearch domain does not have zone awareness enabled, Low) — a single AZ outage takes out every node; `PLERION-AWS-1199` (Auto Scaling group uses a single Availability Zone), which skips scanning appliance groups; and `PLERION-AWS-1200` (VPC routes a subnet through a NAT gateway in another Availability Zone), which skips regional NAT gateways and VPCs without a NAT gateway.

— Four named checks with exact skip conditions, no runnable command

changelog-20261012-dbe0ab06

02 **AWS service quota usage check** NEW 75

Adds `PLERION-AWS-1243` : AWS service quota usage is at or above 80% (Medium), covering EC2 On-Demand Standard vCPUs, Elastic IPs, VPCs per Region, and Lambda concurrent executions, calculated using 24-hour peak CloudWatch usage metrics.

— Named check with threshold, covered resources and metric source

changelog-20261012-dbe0ab06

03 **AgentCore IAM execution role exposure checks** NEW 70

Adds `PLERION-AWS-1201` : AgentCore code interpreter runs with an IAM execution role (Low), flagging custom interpreters where code injection could expose AWS credentials, with the AWS-provided interpreter skipped; and `PLERION-AWS-1202` : AgentCore browser runs with an IAM execution role (Low), flagging browsers where a forged request or malicious page could expose the role's credentials, with the AWS-provided browser skipped.

— Two named checks with clear attack mechanism and exclusions changelog-20261012-dbe0ab06

04 **RDS and EC2 deletion/termination protection checks** NEW

65

Adds `PLERION-AWS-1197` : RDS DB instance does not have deletion protection enabled, where instances inside a cluster are covered by the cluster check and skipped; and `PLERION-AWS-1198` : EC2 instance does not have termination protection enabled, which skips Spot instances and instances in Auto Scaling groups.

— Named checks with exact skip conditions, no severity given changelog-20261012-dbe0ab06

05 **Route 53 failover health check** NEW

60

Adds `PLERION-AWS-1242` : Route 53 hosted zone has a failover record without a health check (Medium) — finds hosted zones whose failover records lack a health check, causing Route 53 to treat the primary as always healthy.

— Single named check with mechanism, no scope/skip detail given

changelog-20261012-dbe0ab06

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

Cloudmersive

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗

RANK

Cloudmersive is a developer API platform offering cloud-based file scanning, malware detection, document conversion, and validation services for integrating security and processing into applications.

> Cloudmersive's Fraud AI API gained a configuration option to control handling of expired documents during validation.

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

01 **Expired document handling in Fraud AI API** IMPROVED

40

The Cloudmersive Fraud AI API `v1-7-0` adds settings to allow or block expired documents during document validation.

— Names API version but no specific flag or field name changelog-20261012-f27eb17b

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Sophos Central

Feedback ⓘ changelog · Oct 12, 2026

CHANGELOG ↗ RANK

Sophos Central is a cloud-based management console for Sophos security products, letting administrators deploy, monitor, and manage endpoint, network, and email protection from one dashboard.

> Sophos Central's latest changelog adds visibility into AI agents and non-human identities created via Microsoft Entra, phishing and DNS protection in Protected Browser, mandatory re-authentication for sensitive Live Response actions, and domain-verification for Dark Web Monitoring, alongside several directory-sync, Wi-Fi, and endpoint-management improvements.

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

01 **Protected Browser phishing, DNS, and deployment updates** NEW

70

Delivers Phishing Protection in Protected Browser to guard organizational credentials, adds direct DNS Protection independent of endpoint or network policies, provides a new MSI installer for easier Windows deployment of Protected Browser, and adds more flexible data boundary controls.

— Names installer and protections but no exact commands changelog-20261012-71fe755f

02 **Policy application status on endpoint page** NEW

70

Shows application status for each policy on the Policies tab of an endpoint's details page, so admins can confirm when an updated policy has taken effect.

Confirm an updated exclusion policy has reached a specific endpoint before assuming it is protected.

> 📍 In Sophos Central, open the endpoint's details page, select the Policies tab, and check the Application status column for the relevant policy to see when the change was applied.

— Exact UI path with a worked example changelog-20261012-71fe755f

03 **Directory sync alerts for Entra ID and Google** NEW

65

Adds alerts for Microsoft Entra ID and Google Directory synchronization — covering successful syncs, warnings, errors, oversized synchronizations, and deactivations — surfaced on the Alerts page.

— Lists alert types and location, no config key changelog-20261012-71fe755f

04 **Dark Web Monitoring domain verification** NEW 60

Adds manual domain entry and DNS TXT record ownership verification for Dark Web Monitoring, removing the requirement to sync domains from Entra ID.

— States mechanism and before/after but no UI steps changelog-20261012-71fe755f

05 **Bulk endpoint actions at scale** IMPROVED 60

Scales bulk endpoint actions on the Computers and servers page to tens of thousands of devices, with long-running actions continuing in the background.

— Names page and scale but no step-by-step changelog-20261012-71fe755f

06 **Entra ID sync scheduling and filtering** IMPROVED 60

Enables scheduling of Entra ID synchronization as frequently as every 30 minutes, with enhanced multi-value operator filtering and selective device-attribute sync.

— States interval and filters but no config path changelog-20261012-71fe755f

THINNER COVERAGE BELOW

07 **Transaction re-authentication for sensitive actions** BREAKING 55

Requires administrators to re-authenticate before running Live Response and sensitive Response Actions via transaction authentication.

— Names triggers but no config toggle detail changelog-20261012-71fe755f

08 **Non-Human Identity visibility for AI agents** NEW 50

Surfaces every AI agent, blueprint, and app created by Microsoft Entra — including owner and sponsor — under Non-Human Identities in the Directory.

— Names the Directory surface but no exact navigation steps changelog-20261012-71fe755f

09 **AP6 MR10 firmware Wi-Fi auth support** NEW 45

Adds AP6 MR10 firmware support for Microsoft Entra ID authentication and Per-SSID RADIUS management.

— Names firmware version but no setup steps changelog-20261012-71fe755f

10 **On-premises AD source deletion in Fusion** NEW 45

Enables deletion of old, unused on-premises Active Directory sources directly from the Sophos Fusion interface.

— Names interface but no exact steps changelog-20261012-71fe755f

WAS THIS USEFUL?  

◆ SIEM

Sumo Logic Feedback ⓘ

Google Workspace Activities (Collection) (2026-10-12) BLOG ↗

Sumo Logic is a cloud-native machine data analytics platform that collects, analyzes, and visualizes logs and metrics for security monitoring, troubleshooting, and operational insights.

NEW INTEGRATION Google Workspace Activities source

WAS THIS USEFUL?  

◆ Detection Engineering

Tenzir

Feedback ⓘ

Tenzir Node v6.20.0-rc.2: A new data model for faster pipelines (2026-10-12)

BLOG ↗ RANK

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

> Tenzir v6.20.0-rc.2 introduces a new data model with heterogeneous lists for faster pipelines, alongside a typed AI decision operator, secrets support in function arguments, new source integrations, and broadened query pushdown across several connectors.

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

01 **Query pushdown across MySQL, SQL Server, SentinelOne, ClickHouse and DuckDB**

IMPROVED 75

Adds filter, projection, and limit pushdown for `MySQL` and `SQL Server` sources; filter and time-window pushdown and queries through the console API for `SentinelOne`; and case-insensitive prefix/suffix filters and regular expression filters in `ClickHouse` and `DuckDB`.

— Multiple named connectors and exact pushdown capabilities

Tenzir Node v6.20.0-rc.2: A new data mo…

02 **`ai_decide` operator for typed decisions** NEW 65

Adds the `ai_decide` operator with typed decisions, paired with new Cloudflare Workers AI and OpenAI Decisions endpoints.

— Named operator and endpoints give a clear starting point

Tenzir Node v6.20.0-rc.2: A new data mo…

03 **Secrets as function arguments** NEW 65

Adds secrets as function arguments, including `secret keys` for `hmac` and `secret seeds` for Crypto-PAn.

— Specific functions named but no usage example Tenzir Node v6.20.0-rc.2: A new data mo…

04 **New collection and storage integrations** NEW 60

Adds Windows Event Forwarding support without requiring a Windows collector, and read and write support for named in-memory `DuckDB` databases.

— Two named integrations, limited mechanism detail

Tenzir Node v6.20.0-rc.2: A new data mo…

THINNER COVERAGE BELOW

05 **New pipeline functions: encryption, checksums, record conversion**

NEW

55

Adds new pipeline functions: encryption functions, a `Luhn` check digit function, a `CRC-32` checksum function, and functions to convert records to key-value entries and record values to a list.

– Functions named but no behaviour detail beyond names

Tenzir Node v6.20.0-rc.2: A new data mo…

06 **Pipeline execution optimizations** IMPROVED

55

Adds narrower input reads for aggregations to reduce data scanned, bounded memory for limited sorting, and the ability for filters to move through assignments and drop and fold constants, improving pipeline efficiency.

– Describes mechanism but not user-facing controls

Tenzir Node v6.20.0-rc.2: A new data mo…

07 **New Suricata schema types** NEW

45

Adds new Suricata schema types for NTP, LDAP, LLMNR, DNP3, drop, and frame events.

– Named event types but no usage context Tenzir Node v6.20.0-rc.2: A new data mo…

08 **New heterogeneous-list data model** NEW

35

Introduces a new data model that allows lists to hold values of different types, and makes pipelines faster overall.

– Explains benefit but no mechanism or named surface

Tenzir Node v6.20.0-rc.2: A new data mo…

09 **Kafka offset test diagnostics** IMPROVED

25

Adds diagnostics for Kafka offset test failures.

– One-line mention with no detail on diagnostic output

Tenzir Node v6.20.0-rc.2: A new data mo…

10 **Best-effort platform pipeline telemetry** NEW

20

Adds best-effort platform pipeline telemetry.

– Bare mention with no mechanism or scope Tenzir Node v6.20.0-rc.2: A new data mo…

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Endpoint Management (UEM/RMM)

Sophos Mobile

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗

Sophos Mobile is an enterprise mobile device management and security platform that secures, manages, and monitors smartphones and tablets for organizations.

Sophos Mobile adds managed Google domain device enrollment for Android Enterprise, enabling Google-based authentication in place of Sophos Fusion.

NEW INTEGRATION Managed Google domain device enrollment

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

Rapid7 InsightVM

Feedback ⓘ changelog · Oct 12, 2026 BLOG ↗

RANK

Rapid7 InsightVM is a vulnerability management platform that scans networks and assets to identify, prioritize, and help remediate security weaknesses.

> InsightVM 8.63.0 adds username visibility to SSH key credential audits and improves the accuracy of CIS policy compliance reporting.

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

01 **Username visibility in SSH key credential audits** IMPROVED

25

SSH key credential audits now display the associated username, giving more context during credential audit reviews.

— Names the capability but no mechanism or UI path given 2026-10-12-751d876f

02 **More accurate CIS policy compliance reporting** IMPROVED

15

InsightVM delivers more accurate CIS policy compliance reporting.

— Only a bare claim, no detail on what changed 2026-10-12-751d876f

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Passbolt

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗

Manage and share passwords securely with Passbolt. Open source, audited and built for teams that need collaboration, compliance and control.

Passbolt 5.16.2 migrates the Microsoft Edge browser extension to Manifest V3, preserving account settings and enabling automatic updates.

UPDATED SUPPORTED PLATFORM Microsoft Edge extension moved to Manifest V3

WAS THIS USEFUL? 👍 👎

SailPoint

Feedback ⓘ

New Capability: SailPoint Oracle Access Governance SaaS Connector (2026-10-12)

BLOG ↗ RANK

SailPoint is an identity governance platform that manages user access, enforces security policies, and automates compliance across enterprise applications and data.

> SailPoint added a new Oracle Access Governance SaaS connector, moved the SAP Concur connector to Spend API V4.1 with a migration flag, and extended Custom User Levels to cover read-only source access.

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

01 SAP Concur connector moves to Spend API V4.1 BREAKING

95

The SAP Concur SaaS & VA connector now supports Spend API V4.1 for Spend User retrieval via a new `useSpendApiV41` application XML config entry, letting admins opt existing sources into V4.1 on their own schedule; sources created on or after June 1, 2026 default to V4.1, replacing the deprecated Spend API V4. V4.1 changes the `customData` response format from label-based field names (V4) to strict camel-case technical field names, so existing `jsonPathMapping` entries that reference `customData` will break and must be reviewed/updated before enabling the flag or before June 1, 2026 for newly created sources.

Opt an existing SAP Concur source (created before June 1, 2026) into Spend API V4.1 after reviewing and updating customData mappings.

xml

```xml
<entry key="useSpendApiV41" value="true"/>

<!-- Updated customData mapping pattern -->
<entry key="orgUnit1" value="
['urn:ietf:params:scim:schemas:extension:spend:2.0:User'].customD
ata[*][?(@.id=='orgUnit1')].value"/>
```

— Named config flag, exact mapping syntax, and runnable example

New Capability: SAP Concur Connector Up…

02 Oracle Access Governance SaaS connector NEW

75

A new Oracle Access Governance (OAG) SaaS connector brings OAG identities, roles, and access bundles into SailPoint Identity Security governance, aggregating OAG identities as accounts and OAG roles/access bundles as entitlements with application-

level and included-permission context. It supports access requests, grants, and revocations through the Identity Security request center (forwarding approved requests to OAG for fulfillment, with clear results when an OAG guardrail or segregation-of-duties check blocks a request), plus lifecycle operations — activating, terminating, enabling, disabling, and deleting OAG identities and downstream Oracle accounts — with per-application lifecycle controls to target a specific Oracle application without affecting others.

— Detailed mechanism and scope, but no CLI/API example given

New Capability: SailPoint Oracle Access…

THINNER COVERAGE BELOW

03 **Read Only access level for Sources** IMPROVED 35

Custom User Levels in SailPoint Identity Security Cloud now support Read Only permissions on Sources, letting admins grant scoped source visibility to operators, support, and audit users without granting full access.

— States what changed but no config key or UI path given

Enhancement: Custom User Level - Read O…

└──▷ **BREAKING ON UPGRADE**

! Existing `jsonPathMapping` entries that reference `customData` labels will break under Spend API V4.1: V4.1 returns strict camel-case technical field names instead of the human-readable labels returned by V4. Mappings must be reviewed and updated before enabling `useSpendApiV41` or before June 1, 2026 for sources created after that date.

WAS THIS USEFUL? 👍 👎

◆ Backup & Recovery

Commvault Cloud

Feedback ⓘ changelog · Oct 1, 2026 NOTES ↗

RANK

Commvault Cloud is a backup, recovery, and cyber-resilience platform for hybrid, multi-cloud, and SaaS workloads.

> Commvault Cloud 11.46 adds real-time Active Directory auditing with rollback, expands database and VM protection (Redis/Valkey, YugabyteDB, MongoDB Atlas, XenServer/Proxmox CBT, VDDK 9.1/VCF), and strengthens cloud-native integration with GCP service account impersonation, a first-party Azure portal integration, and availability in the AWS European Sovereign Cloud region.

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

01 **Real-time AD auditing and anomaly detection** NEW 70

Captures identity, group, policy, and authentication changes with automatic highlighting of privilege escalations, delegation updates, and policy modifications; supports rollback of directory changes directly from the audit event. Requires Active Directory Advanced Edition license.

— Names license requirement and rollback action, no exact command 2026-10-01-46c624d8

02 **New database support: Memorystore Redis/Valkey, YugabyteDB, MongoDB Atlas**

NEW 65

Adds support for Google Cloud Memorystore for Redis and Valkey backup and recovery within Commvault, YugabyteDB protection for Google Cloud deployments covering YSQL databases and YCQL keyspaces through the unified Commvault platform, and MongoDB Atlas native snapshot onboarding and management in SaaS.

— Names every new provider and workload type precisely 2026-10-01-46c624d8

03 **Changed Block Tracking for XenServer and Proxmox VE** NEW 60

Adds Changed Block Tracking (CBT) support for incremental VM backups on XenServer and Proxmox VE, reducing backup windows, data transfer, and resource utilization.

— Explains benefit and targets but no setup steps 2026-10-01-46c624d8

04 **GCP service account impersonation for credential isolation**

NEW 60

Adds Google Cloud service account impersonation for credential isolation, using project-specific short-lived tokens scoped to discovery, backup, restore, and storage operations for database workloads, and for VM backup and restore jobs, reducing cross-project permission sprawl and improving per-project auditability.

— Explains mechanism but no config or flag named `2026-10-01-46c624d8`

05 **NetApp StorageGRID Change Detection API support** NEW 60

Adds NetApp StorageGRID Change Detection API support for accelerated incremental scanning, focusing only on modified objects to reduce scan time and resource consumption.

— Names the API but no endpoint or flag given `2026-10-01-46c624d8`

06 **OCI VM recovery with automatic NSG mapping** NEW 60

Adds OCI VM recovery with automatic Network Security Group (NSG) mapping, pre-populating NSG selections during restore from metadata captured at backup time.

— Explains mechanism, no exact UI/command given `2026-10-01-46c624d8`

THINNER COVERAGE BELOW

07 **Native Commvault integration as first-party Azure resource** NEW 50

Adds native Commvault integration as a first-party Azure resource within the Azure portal, enabling protection, management, and recovery of Azure workloads without leaving the portal.

— Names Azure portal as entry point, lacks deeper mechanism `2026-10-01-46c624d8`

08 **VMware VDDK 9.1 and VCF support** NEW 45

Adds VMware VDDK 9.1 support and extends protection to VM workloads on vCenter Servers deployed through VMware Cloud Foundation (VCF).

— Names versions but no setup steps `2026-10-01-46c624d8`

09 **Availability in AWS European Sovereign Cloud region** NEW 45

Adds Commvault Cloud availability in the AWS European Sovereign Cloud (ESC) region, keeping backup data, metadata, and recovery operations within EU sovereign boundaries.

— Names region but no activation steps `2026-10-01-46c624d8`

10 **Search-driven recovery for object storage** NEW 35

Adds a search-driven recovery experience for object storage, allowing customers to find and restore specific items without navigating large datasets.

— Thin description with no named surface or steps `2026-10-01-46c624d8`

WAS THIS USEFUL? 👍 👎

INFRASTRUCTURE

◆ Internet Services

Cloudflare

Feedback ⓘ changelog · Oct 12, 2026 CHANGELOG ↗

RANK

Cloudflare is a connectivity cloud platform delivering internet security, performance, and developer infrastructure services.

> Cloudflare's Agents SDK gained built-in web_fetch/web_search tools and an experimental OpenCode runtime, while Queues added jurisdictional data residency, API Shield gained on-demand schema learning, and Markdown for Agents raised its size limit at the cost of two response headers.

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

01 **web_fetch and web_search tools in Agents SDK** NEW 90

Agents SDK v0.28.0+ adds `web_fetch` (importable from `agents/webfetch/pi`) for reading webpages, PDFs, and supported Office documents with automatic Markdown conversion, exposing fetchWeb(), windowWebFetchPage(), and renderWebFetchPage() for direct fetching without a model or Durable Object. Agents SDK v0.27.0+ adds `web_search` (importable from `agents/websearch/pi`) for querying the public web via the Cloudflare Web Search API (powered by ceramic.ai, Exa, and Linkup), exposing createAIWebSearch() and createHTTPWebSearch() for model-free search.

— Names functions, import paths and versions; no runnable example

changelog-20261012-8c3397f0

02 **Jurisdictional restrictions for Cloudflare Queues** NEW 90

Adds jurisdictional restrictions to Cloudflare Queues via the `--jurisdiction` flag (Wrangler) and `jurisdiction` parameter on the `POST /queues` API endpoint; supported values are `eu` (European Union), `us` (United States), and `fedramp` (FedRAMP-Moderate data centers).

Create a GDPR-compliant Cloudflare Queue that stores and processes messages only within the EU, during initial queue provisioning.

```
$ wrangler queues create --queue-name my-eu-queue --jurisdiction
eu
```

Provision an EU-jurisdiction queue via the API, for automated infrastructure pipelines.

```
$ curl -X POST
https://api.cloudflare.com/client/v4/accounts/<account_id>/queues
\
  -H 'Authorization: Bearer <token>' \
  -H 'Content-Type: application/json' \
  -d '{"queue_name": "my-eu-queue", "jurisdiction": "eu"}'
```

— Runnable Wrangler and API examples provided `changelog-20261012-8c3397f0`

03 **OpenCodeHarness for running OpenCode in a Durable Object** NEW

85

Adds `OpenCodeHarness` (experimental) to the Agents SDK, enabling OpenCode 2.0 to run inside a plain Durable Object with SQLite sessions, Lifecycle jobs, and Workers AI model binding via the `agents/models/opencode` provider; requires `agents@latest @opencode/sdk@2 @opencode/plugin@2`.

— Names provider and install requirement, no usage example `changelog-20261012-8c3397f0`

04 **Larger HTML limit and streaming for Markdown for Agents**

70

BREAKING

Raises the Markdown for Agents HTML conversion limit from 2 MiB to 6 MiB (6,291,456 bytes) of decompressed HTML, and switches to an in-process streaming engine at the edge. Converted responses no longer emit the `x-markdown-tokens` and `x-original-tokens` headers (clients must calculate token counts themselves), and `Content-Length` is removed from responses since the body is now streamed.

— Gives exact limits and removed headers, no migration code `changelog-20261012-8c3397f0`

THINNER COVERAGE BELOW

05 **Extended grace period for Workers runtime updates** IMPROVED

50

Extends the Workers runtime update grace period for pending requests and connections from 30 seconds to up to 20 minutes, covering long-running HTTP requests, streamed AI responses, and live WebSocket sessions.

— Clear before/after numbers, but nothing for reader to act on

`changelog-20261012-8c3397f0`

06 **Unified navigation combining Zero Trust and main dashboard**

IMPROVED

45

Zero Trust customers now get a single sidebar combining Zero Trust and main Cloudflare dashboard navigation, gaining access to developer platform, account memberships, and

resource tagging. Zero Trust Network items are replaced by experiences under `Networking`, and Resolvers & Proxies moved under Traffic Controls.

— Describes the change but gives no exact navigation path `changelog-20261012-8c3397f0`

└──▷ ALSO FROM THESE RELEASES

.
.
.

└──▷ BREAKING ON UPGRADE

! Converted Markdown for Agents responses no longer emit the `x-markdown-tokens` and `x-original-tokens` headers; clients that relied on these values must calculate token counts themselves.

! `Content-Length` is removed from Markdown for Agents converted responses (the body is now streamed); clients that depended on this header must handle its absence.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 12, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue