THE CYBER TOOLCHAIN

NO. 071

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 11, 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 189 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 35 tools

▾ // THE BRIEF HIDE SAME ISSUE, SAME PROMPT, TWO WRITERS: GPT-5.5 Opus 5

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

Three unrelated things stand out today: JumpCloud tightened identity and AI access with GA risk detection and scoped MCP servers; Tenzir

vim ? help

made Microsoft security telemetry cheaper to ingest and normalize; Prowler made restricted and air-gapped cloud scanning less brittle.

GOVERN

Keep AI tool access inside identity policy

JumpCloud now requires MCP servers in AI Gateway to be scoped to SSO applications, while ConductorOne added governance for MCP server resources. That moves AI-agent tool access out of ad hoc configuration and into the same reviewable access paths teams already use for apps and entitlements.

JumpCloud · ConductorOne

DETECT

Pull Microsoft telemetry into the pipeline with less glue code

Tenzir added Microsoft 365, Microsoft Defender, and Azure Log Analytics sources, plus automatic OCSF matching for sigma rules. Teams can route those logs into detection content without hand-building as much ingestion and field-normalization plumbing first.

Tenzir

PROTECT

Scan and prioritize vulnerabilities when networks cannot freely reach the internet

Prowler added AWS ISO partition support, configurable Boto3 timeouts, and a persistent Trivy vulnerability database cache for air-gapped image scanning. CVE MCP Server debuted a `triage_cve` orchestrator that pulls NVD, EPSS, CISA KEV and PoC sources into a composite risk score and SSVC v2 decision, cutting down the manual lookup work behind patch prioritization.

Prowler · CVE MCP Server

PROTECT

Separate maintenance freezes from visibility gaps

Automox can now block Policy Execution and Device Scans independently inside Exclusion Windows, with API support, UI indicators, and audit logging. Teams can pause change-making activity during sensitive windows without also losing scan visibility by default.

Automox

Does **GPT-5.5** read better? 👍 👎

OFFENSIVE SECURITY

◆ Wireless & RF

Bastille Networks

Feedback ⓘ 1 RELEASE · SEEN 2026-09-11

PRESS ↗ RANK

Bastille is the leading wireless intrusion detection system (WIDS), helping enterprises and AI data centers secure their wireless airspace.

> Bastille added smart glasses detection and precise location to its wireless intrusion detection platform, delivered as a software update to existing customers.

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

01 **Smart glasses detection and location** NEW 60

Bastille now identifies the unique wireless signatures of smart glasses within seconds of their entry into a monitored facility, and locates them to within one to three meters in real time across Wi-Fi, Bluetooth, and cellular frequencies. Detections automatically alert security teams and feed into existing security systems with no new infrastructure required, delivered to existing customers via a subscription software update requiring no hardware changes.

— Explains mechanism and precision but lacks specific commands or config.

launch-20260911-495f8c09

WAS THIS USEFUL? 👍 👎

fluxion

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗ RANK

Fluxion is a remake of linset by vk496 with enhanced functionality.

> Fluxion v6.32 swaps the Captive Portal attack's DHCP backend from isc-dhcp-server to kea-dhcp4, changing config generation, AppArmor handling, and the lease file location.

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

01 Captive Portal DHCP backend switched to kea-dhcp4

BREAKING

75

The Captive Portal attack's DHCP backend is replaced, moving from `isc-dhcp-server` (`dhcpd`) to `kea-dhcp4` , with JSON-based config generation and AppArmor local override handling for the `kea-dhcp4` profile. Systems relying on `isc-dhcp-server` will need `kea-dhcp4` installed and its AppArmor profile configured.

— Names exact backend, config format and AppArmor profile change v6.32

02 DHCP lease file relocated to kea CSV format

BREAKING

65

The DHCP lease file has moved to `/var/lib/kea/kea-leases4.csv` , and client IP/MAC/hostname lookup has been reworked against kea's CSV lease format. Tooling or scripts reading the old `dhcpd` lease file path will no longer find client lease data there.

— Exact new file path given but no lookup mechanism detail v6.32

└──▷ **BREAKING ON UPGRADE**

! The DHCP backend for the Captive Portal attack is replaced by `kea-dhcp4` ; systems relying on `isc-dhcp-server` (`dhcpd`) will need `kea-dhcp4` installed and its AppArmor profile configured.

! The DHCP lease file has moved to `/var/lib/kea/kea-leases4.csv` ; any tooling or scripts that read the old `dhcpd` lease file path will no longer find client lease data there.

WAS THIS USEFUL? 👍 👎

◆ Reconnaissance & OSINT

Nmap

Feedback ⓘ changes since 2026-09-06 CODE ↗

Nmap - the Network Mapper. Github mirror of official SVN repository.

Nmap NSE gains rudimentary 802.1Q / 802.1ad VLAN tag support for parsing and building tagged Ethernet frames.

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-09-06
https://github.com/nmap/nmap.git
# already have the repo? check out this version:
$ git checkout commits-2026-09-06
```

Adds `frame.vlans` list to packet.Frame:new(), populated with per-tag tables containing `tpid`, `pcp`, `dei`, and `vid` fields when 802.1Q (`0x8100`) or 802.1ad (`0x88a8`) tags are present.

Extends packet.Frame:build_ether_frame() with an optional VLAN list parameter to construct 802.1Q / 802.1ad tagged Ethernet headers from NSE scripts.

Adds `ETHER_TYPE_8021Q` and `ETHER_TYPE_8021AD` constants to the NSE packet library for use in script-level Ethernet type comparisons.

Updates the pcap capture path to correctly skip multiple stacked 802.1Q / 802.1ad VLAN tags when computing L3 offsets, enabling NSE scripts to operate on traffic from tagged (trunk) network segments.

WAS THIS USEFUL? 👍 👎

◆ AI-Powered Offensive Security

Dreadnode

Feedback ⓘ 3 RELEASES · 2026-08-27 → 2026-09-10 NOTES ↗

RANK

Documentation for the Dreadnode AI security platform — self-hosting guides, platform concepts, SDK reference, and CLI documentation.

> Dreadnode expanded its AI red-teaming surface with a dozen new multi-agent tasks, honeytoken and attack-success-detection tooling, and traditional ML attack targets now open to all organizations, alongside a Global Tool Registry API, full air-gapped/offline deployment support, and a run of web-security capability additions (HTTP desync detection, geo-DNS, IP rotation, LSB steganography).

└──▷ WHAT SHIPPED · 31 FEATURES most completely described first ? what's the number?

01 CLI and TUI usability improvements NEW

90

Adds `DREADNODE_TUI_THEME=light` to switch the TUI from its default dark palette to a light theme; `/reload` to reload the current agent without leaving a chat session; `/transcript` to toggle between compact and full agent transcript views; and `/status` to show the current session, model, user, org, workspace, and project at a glance. The CLI adds a `--mine` flag to `dn runtime ls` to filter to runtimes you own (and marks non-owned runtimes in the default listing) and a `provision` alias for `create` in `dreadnode env`.

Check your current session context at a glance in the TUI without leaving the chat interface.

```
$ /status
```

List only the runtimes you own to avoid acting on a colleague's shared runtime in a multi-user workspace.

```
$ dn runtime ls --mine
```

— Names every flag and command verbatim; fully actionable.

Traditional ML attack targets now avail… Web Chat open to all users

02 Global Tool Registry API NEW

90

Adds `GET /api/v1/tools` and `GET /api/v1/tools/{tool_id}` endpoints to query the new Global Tool Registry, giving published capability Python tools and command wrappers stable, organization-scoped identities with immutable revision history.

Enumerate all registered tools in your organization to audit capability surface before a red-team engagement.

```
$ curl -s -H 'Authorization: Bearer <token>' https://<your-instance>/api/v1/tools | jq '.[].id'
```

— Named endpoints with methods, plus a runnable query example.

Offline SDK and CLI install for air-gap…

03 **Air-gapped and offline deployment support** NEW 90

Serves the SDK and CLI as self-contained offline bundles from self-hosted deployments (no PyPI or external host required) and serves documentation at `/docs` inside every deployment. Adds an air-gap deployment mode that vendors all front-end resources locally, hides the analytics notebook, serves model pricing from a bundled catalog, and pre-bakes capability dependencies into the runtime image so sandbox boot requires no network access, plus a `replicated.isAirgap=true` Helm setting to stop the Replicated SDK pod reaching `replicated.app`.

Prevent the Replicated SDK pod from phoning home during a Helm-based air-gap install in a disconnected environment.

```
$ helm upgrade --install dreadnode ./dreadnode-chart --set replicated.isAirgap=true
```

— Names config flag, doc path, and mechanisms across two releases.

Offline SDK and CLI install for air-gap… Web Chat open to all users

04 **Runtime cold-start performance and timing diagnostics**

IMPROVED 85

Runtime cold start was reduced by more than 60%, dropping time-to-ready from 18.8 s to 6.6 s, and `dn runtime start` and `GET /runtimes/{id}` now surface a full timing breakdown (total, platform overhead, provider provisioning, boot, installs, slowest step).

Inspect the cold-start timing breakdown on a slow runtime to attribute whether delay is provider provisioning or package install.

```
$ dn runtime start && curl -s -H 'Authorization: Bearer <token>'
https://<your-instance>/runtimes/<id> | jq '.timing'
```

— Exact before/after numbers plus command and endpoint to inspect.

Traditional ML attack targets now avail… | Offline SDK and CLI install for air-gap…

---

05 **Traditional ML attack targets across all organizations** NEW

75

Three traditional ML attack targets — `fraud tabular`, MNIST image, and IMDB text — are now available to all organizations, covering extraction, membership inference, evasion, and inversion attack types, and are provisionable by name via the SDK or TUI, including bare public task name resolution without an org prefix.

Provision a public ML attack target by bare task name — no org prefix required — to kick off a membership inference campaign.

```
$ dreadnode env provision ml-extraction-fraud-tabular
```

— Names targets and attack types with a runnable provisioning example.

Traditional ML attack targets now avail…

---

06 **CA trust and Helm chart hardening for self-hosted deployments**

IMPROVED

75

Adds a `caBundle` config key for self-hosted deployments to inject a custom CA bundle into the Node frontend, completing CA trust support across all workloads (API, LiteLLM, and frontend); Helm charts also gain support for non-root container execution and custom CA bundle mounts for outbound TLS trust in private-CA environments.

Inject an internal CA into the Node frontend on a self-hosted air-gapped deployment so TLS to an on-prem model proxy is trusted.

```yaml
caBundle: |
  -----BEGIN CERTIFICATE-----
  <your-internal-CA-cert>
  -----END CERTIFICATE-----
```

— Names the exact config key and shows a values.yaml example.

Offline SDK and CLI install for air-gap… | Web Chat open to all users

---

07 **Indirect prompt injection web task** NEW

70

Adds an indirect prompt injection web task where agents must detect injections hidden via HTML comments, hidden CSS, off-screen ARIA, white-on-white text, and Unicode tags across a public web page.

— Concrete injection vectors named but no task ID or run command.

Offline SDK and CLI install for air-gap…

08 **Environment-agnostic attack-success detection in airt SDK**

NEW 70

Adds environment-agnostic attack-success detection to the `airt` SDK, using canary exfiltration, OAST beacons, dataflow taint, LLM judge scoring, and optional customer-defined success policies to produce confidence-rated verdicts.

— Names detection mechanisms in detail, no exact API call shown.

Offline SDK and CLI install for air-gap…

09 **Cloudflare Workers OAST support in web-security capability**

NEW 70

Adds Cloudflare Workers support via `wrangler` to the web-security capability for deploying programmable OAST endpoints, enabling blind XSS payload hosting, callback logging, and SSRF chain redirection.

— Names the tool and three use cases, no exact command shown.

Offline SDK and CLI install for air-gap…

10 **postMessage handler detection expansion** IMPROVED 70

Expands `postMessage` handler detection in the web-security capability's DOM analysis to cover `window.onmessage`, `MessagePort` / `MessageChannel`, and monitoring-shim wrappers, plus additional origin-validation bypass patterns including unescaped-dot and missing-anchor regex bugs.

— Names exact APIs and bypass bug classes covered. Web Chat open to all users

11 **Bulk workspace and session admin actions** NEW 65

Adds bulk workspace member addition to select and add multiple members to a workspace at once from the workspace settings page; a bulk share-with-workspace action for multiple agent sessions via the floating action bar; and bulk archive and unarchive for agent sessions from the Sessions tab, with context-aware actions for active, archived, or mixed selections.

— Names UI locations for each bulk action across three releases.

Traditional ML attack targets now avail… Offline SDK and CLI install for air-gap… Web Chat open to all users

12 **workspace_mount runtime option becomes a no-op** BREAKING

65

The `workspace_mount` runtime option is now a no-op; `/home/user/workspace` is ordinary sandbox-local storage, and object-storage access must go through the SDK instead.

– Clear before/after and required migration path via SDK.

Traditional ML attack targets now avail…

13 **Multi-agent AI red-teaming task catalog expansion** NEW

65

Adds 12 multi-agent AI red-teaming tasks covering access-control bypass, indirect injection, memory poisoning, MCP poisoning, reasoning hijack, supply-chain, data exfiltration, DevOps RCE, and sector-specific meshes to the task catalog under the `airt-generative-ai` set.

– Names the task set and attack categories but not individual tasks.

Offline SDK and CLI install for air-gap…

14 **HTTP desync and request-smuggling detection** NEW 65

Adds HTTP desync and request-smuggling detection to the web-security capability, covering 11 smuggling families with fingerprinting, payload construction, cache-poisoning detection, and victim-response classification.

– Names family count and detection stages, no run command. Web Chat open to all users

15 **Geo-distributed DNS resolution in web-security capability** NEW 65

Adds geo-distributed DNS resolution to the web-security capability, resolving target hostnames through open resolvers in multiple countries (via Shodan or Censys) to detect geo-fenced infrastructure, GSLB routing, and region-locked DNS responses.

– Names data sources and detection targets, no exact tool command.

Web Chat open to all users

16 **Signup IP allow-list mode** NEW 60

Adds signup IP allow-list mode letting admins restrict new account creation to explicitly approved IPv4/IPv6 CIDR ranges, with deny rules taking precedence over allow rules.

– Describes the mechanism but no exact admin UI or config path.

Offline SDK and CLI install for air-gap…

17 **Honeytoken canary tools in AI red-teaming capability** NEW

60

Adds two honeytoken tools to the `ai-red-teaming` capability: one to mint canary tokens (exfil or RCE variants) and one to check whether a target agent leaked them across an output boundary.

– Names the capability and both tool functions, no exact command.

Offline SDK and CLI install for air-gap…

18 **SDK transforms and scorers for exfiltration and browser attacks**

NEW 60

Adds SDK transforms and scorers covering search-query and trusted-domain image exfiltration channels, plus dedicated browser-attack scorers for visual injection, ClickFix execution, navigation hijacking, and domain-validation bypass.

– Names scorer categories but no function names or usage.

Offline SDK and CLI install for air-gap…

19 **Failed capability preflight checks surfaced as warnings**

IMPROVED 60

Surfaces failed capability preflight checks (e.g. missing `dnsx`, `katana`) as explicit warnings in the agent system prompt and operator logs instead of silently proceeding.

– Names example missing tools and where warnings surface. Web Chat open to all users

THINNER COVERAGE BELOW

20 **New Account Settings sections** NEW 55

Adds a Release Notes section in Account Settings listing the ten most recent changelog entries with links to full docs, available on both SaaS and self-hosted installs, plus a direct link to the system status page in the Support tab of Account Settings on SaaS deployments.

– UI-only additions with clear navigation but no deeper mechanism.

Traditional ML attack targets now avail…

21 **Session list search and pagination** IMPROVED 55

Adds pagination and full-text search by title, model, agent, and label to the chat session list, removing the previous 100-session cap.

– Names searchable fields and the removed cap, no exact endpoint.

Web Chat open to all users

22 **Agentic CI/CD secret-exfiltration task** NEW 55

Adds an agentic CI/CD secret-exfiltration multi-agent task simulating hidden instructions in untrusted repo content that cause a CI assistant to leak its deploy secret.

– Clear scenario but no task identifier to invoke it.

Offline SDK and CLI install for air-gap…

23 **Multi-step tool attack sandbox task** NEW 55

Adds a multi-step tool attack sandbox task featuring an over-permissioned agent with file, database, email, and HTTP tools, where success requires chaining a sensitive data source to an external exfiltration sink.

– Describes the attack chain but no task name to run it.

Offline SDK and CLI install for air-gap…

24 **Algorithmic multi-step tool-attack search** NEW 55

Adds algorithmic multi-step tool-attack search to the AI red-teaming agent for finding replay-stable read-then-exfiltrate causal paths across HTTP agent tool call chains.

– Explains the search goal but no invocation surface.

Offline SDK and CLI install for air-gap…

25 **IP rotation tool in web-security capability** NEW 55

Adds an IP rotation tool to the web-security capability, deploying Cloudflare Worker proxies on demand for round-robin egress through rotating IPs during engagements.

– Explains mechanism but no invocation command. Web Chat open to all users

26 **LSB steganography support in web-security capability** NEW 55

Adds LSB steganography support for PNG images to the web-security capability, enabling payload-smuggling tests and upload pipeline inspection via the built-in Python tool.

– Names format and use case but not the tool's exact name. Web Chat open to all users

27 **Lifetime credit cap per non-owner member** NEW 50

Adds an organization-owner-configurable lifetime credit cap per non-owner member, visible to capped members under Settings → Billing.

– Names the settings location but no config key or limit value.

Offline SDK and CLI install for air-gap…

28 **OWASP-ASI attack suite runner and tool-evidence scoring in SDK**

NEW 50

Adds a turnkey OWASP-ASI agentic attack suite runner, argument-aware tool-evidence scoring, and a honeytoken harness for black-box exfil and RCE detection to the SDK.

– Names three SDK additions but no function or class names.

Offline SDK and CLI install for air-gap…

29 **Attribution and metadata for sessions and assessments** NEW 45

Session responses now include attribution for who shared a session with the workspace and when, covering all share paths including bulk promotion and creation-time visibility; AIRT assessments and findings now display the workspace member who ran each assessment; and each session in the chat session list now displays a message count.

— Explains scope of attribution but no API or field names.

Traditional ML attack targets now avail…

30 **Capability credential visibility before install** IMPROVED

35

The capability detail view and install picker now display which credentials a capability requires before installation.

— Describes the change but no named fields or flow detail.

Traditional ML attack targets now avail…

31 **Guard invocation highlighting in session transcripts** NEW

35

Adds guard invocation highlighting in session transcripts, showing policy decisions inline within the conversation view.

— States the behaviour but no mechanism for how guards are evaluated.

Web Chat open to all users

└──▷ **BREAKING ON UPGRADE**

! The `workspace_mount` runtime option is now a no-op; `/home/user/workspace` is ordinary sandbox-local storage. Object-storage access must go through the SDK.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

ZeroPath

Feedback ⓘ 1 RELEASE · 2026-09-11 CHANGELOG ↗ RANK

ZeroPath is an AI-native SAST platform that finds 2x more real vulnerabilities with 75% fewer false positives.

> ZeroPath added Gerrit code review scanning, a Streamable HTTP MCP server for AI coding assistants, Microsoft Teams channel notifications, and administrator-authored Assistant Skills, alongside access sync for GitHub and Bitbucket teams and a tenfold increase in per-scan validation capacity.

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

01 **Access sync for GitHub and Bitbucket teams** NEW 75

Adds access sync for GitHub and Bitbucket teams, including Bitbucket Cloud workspace groups and Bitbucket Server project groups, mapping provider roles to 39 ZeroPath permissions across 10 groups.

— Gives exact permission and group counts but no config step. changelog-20260911-ed06a3ad

02 **Assistant Skills for methodology customization** NEW 70

Adds Assistant Skills: reusable, administrator-authored methodology files covering triage, dependency reachability, report writing, and patch review that guide the Assistant's behavior. Four built-in skills ship forkable, and edits apply starting on the next run.

— Names all four skill types and the fork/apply mechanism. changelog-20260911-ed06a3ad

03 **Gerrit project scanning** NEW 65

Adds Gerrit project scanning with both full scans and per-patch-set scanning of open changes; findings are posted as review messages directly on the patch set.

— Describes scan modes and output surface but no config key. changelog-20260911-ed06a3ad

THINNER COVERAGE BELOW

04 **Broader language coverage for analysis-depth sizing** IMPROVED 55

Terraform, Svelte, Vue, Solidity, Elixir, Dart, protobuf, and Genero now count toward repository size when ZeroPath decides analysis depth.

— Names all eight languages but the change is automatic, not actionable.

changelog-20260911-ed06a3ad

05 **Jira and Linear ticket creation permission** NEW 50

Adds Jira and Linear ticket creation as a per-repository permission; organizations using access control must grant it explicitly before users can create tickets.

— Names the two integrations and the permission-grant step. changelog-20260911-ed06a3ad

06 **Select-all applies to full filtered findings set** IMPROVED 45

Select-all across pages now acts on the full filtered findings set, so bulk triage applies to exactly the displayed results instead of just the current page.

— Clear UI behavior change but no exact navigation given. changelog-20260911-ed06a3ad

07 **Hardcoded-credential redaction and CWE classification** IMPROVED 35

Hardcoded-credential findings are now redacted on every surface and classified by CWE.

— States the change but no mechanism or scope detail. changelog-20260911-ed06a3ad

08 **Security posture endpoint omits placeholder values** IMPROVED 35

Eleven measurements on the security posture endpoint now return no value, instead of a placeholder, where there is nothing to measure.

— Notes the count of affected measurements but not the endpoint path.

changelog-20260911-ed06a3ad

└──▷ **BREAKING ON UPGRADE**

! On repository objects, `lastScanError` is replaced by `lastScanFailure`; any integration reading `lastScanError` will receive no data after upgrade.

WAS THIS USEFUL? 👍 👎

GitHub

Feedback ⓘ 4 RELEASES · 2026-09-10 BLOG ↗ RANK

Join the world's most widely adopted, AI-powered developer platform where millions of developers, businesses, and the largest open source community build software that advances humanity.

> GitHub shipped a public-preview refresh of the pull request listing page, new REST endpoints to manage AI Scan for pull requests at scale, granular `cache-mode` controls for Actions cache access, and an macOS 27 upgrade for the xcode-27 runner images.

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

01 **cache-mode for Actions cache access control** NEW 93

GitHub Actions adds `cache-mode` to control least-privilege access to the Actions cache at workflow and job level: job-level settings override workflow-level ones, and a called reusable workflow cannot receive more cache access than its caller granted. Setting `cache-mode` explicitly to `write` or `write-only` on low-trust events such as `pull_request_target` (where the default is `read`) now triggers a warning annotation.

Lock a PR workflow to read-only cache access to prevent a contributor's code from poisoning the cache used by trusted builds.

yaml

```yaml
on:
  pull_request:

permissions:
  contents: read

cache-mode: read

jobs:
  build:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - uses: actions/cache@v4
        with:
          path: ~/.npm
          key: ${{ runner.os }}-node-${{ hashFiles('**/package-lock.json') }}
      - run: npm ci
```

Allow a deployment job to save a freshly built artifact to the cache while preventing it from restoring — useful when you want to seed the cache without consuming a potentially tainted entry.

```yaml
on:
  push:
    branches: [main]

jobs:
  seed-cache:
    runs-on: ubuntu-latest
    cache-mode: write-only
    steps:
      - uses: actions/checkout@v4
      - uses: actions/cache@v4
        with:
          path: dist/
          key: ${{ runner.os }}-dist-${{ github.sha }}
      - run: npm run build
```

— Names the config key, its values, defaults, and shows runnable YAML

Control GitHub Actions cache access wit…

02 **AI Scan for pull requests REST API** NEW 90

New `GET` / `PATCH` endpoints on `/orgs/{org}/code-scanning/ai-scan` and `/repos/{owner}/{repo}/code-scanning/ai-scan` let you read and update AI Scan for pull requests enablement at the organization or repository level, enabling programmatic at-scale rollout of AI-powered security detections without configuring each repo in the UI. In public preview.

Enable AI Scan for pull requests on a specific repository without touching the GitHub UI.

```
$ curl -X PATCH \
  -H 'Authorization: Bearer <token>' \
  -H 'Accept: application/vnd.github+json' \
  -d '{"enabled": true}' \
  https://api.github.com/repos/{owner}/{repo}/code-scanning/ai-scan
```

Check whether AI Scan for pull requests is enabled at the organization level before rolling out to individual repos.

```
$ curl -X GET \
  -H 'Authorization: Bearer <token>' \
  -H 'Accept: application/vnd.github+json' \
  https://api.github.com/orgs/{org}/code-scanning/ai-scan
```

— Exact endpoints with methods and runnable curl examples

AI Scan for pull request APIs in public…

03 **Refreshed pull requests listing page** NEW 75

A public-preview redesign of the repository PR listing page adds content assist to help find and apply filters, advanced search supporting `AND` / `OR` keywords and nested searches, a collapsible sidebar with quick-access filters like Authored by me and Involves me, a compact presentation mode to fit more PRs on screen, and richer per-PR context including status check counts, stack indicator, and unread-update indicators. Opt in via the Preview badge at the top of the pull requests tab, and switch back to the classic view the same way.

Opt in to the refreshed PR listing page and switch back to the classic view if needed.

> 📍 1. Navigate to the pull requests tab of any repository. 2. Click the Preview badge at the top of the page to enter the refreshed experience. 3. To return to the classic view, click the Preview badge again and choose Switch back.

— Names every constituent addition and gives exact opt-in steps

Refreshed repository pull requests page…

THINNER COVERAGE BELOW

04 **xcode-27 runner image on macOS 27** IMPROVED 50

The GitHub-hosted `xcode-27` and `xcode-27-xlarge` runner images are upgraded to run on macOS 27, up from macOS 26, enabling Apple app validation against the latest OS on arm64 runners. Public preview.

— States the upgrade but gives no usage steps beyond the image name

Xcode 27 runner image now runs on macOS…

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

Bitnami Sealed Secrets

Feedback ⓘ 1 RELEASE · 2026-09-10

NOTES ↗ CODE ↗ RANK

A Kubernetes controller and tool for one-way encrypted Secrets

> Sealed Secrets added support for omitting encrypted keys via null values and hardened the rotate endpoint against decryption oracle abuse.

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

01 **Omit encrypted keys via null** NEW 60

`encryptedData` keys can now be omitted from the unsealed Secret by setting the corresponding key to `null` in the SealedSecret template.

— Names exact config field and mechanism helm-v2.20.0

THINNER COVERAGE BELOW

02 **Hardened `/v1/rotate` endpoint** IMPROVED 35

The `/v1/rotate` endpoint was hardened against decryption oracle abuse, per the helm-v2.20.0 release summary.

— Names endpoint but no mechanism detail helm-v2.20.0

WAS THIS USEFUL? 👍 👎

infisical

Feedback

1 RELEASE · 2026-09-11

NOTES ↗

RANK

Infisical is the open-source platform for secrets, certificates, and privileged access management.

> Infisical v0.165.10 revamps the secret validation rule API, adds certificate profile attachment for imported PKI certificates, and supports folder creation during vault migration.

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

01 **Certificate profile attachment for imported certs** NEW

37

Supports attaching a certificate profile to imported certificates in PKI, enabling policy-driven management of externally sourced certs.

— Describes benefit but no UI path or API given v0.165.10

02 **Folder creation in vault migration** IMPROVED

37

Adds folder creation support to the vault migration feature, allowing secrets to be migrated into a structured folder hierarchy.

— Explains behaviour but no command or flag named v0.165.10

03 **Validation rule API revamp** IMPROVED

30

Revamps the validation rule API, enabling updated programmatic control over secret validation rules.

— Names the API area but no endpoints or fields given v0.165.10

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

OWASP ZAP

Feedback ⓘ 1 RELEASE · 2026-09-08 BLOG ↗ RANK

The ZAP by Checkmarx Core project

> OWASP ZAP's August 2026 update centers on a new LLM Support add-on connecting ZAP to Claude, Gemini, Azure OpenAI, Ollama and OpenAI-compatible endpoints, alongside new MCP Integration tools, a shared `maxMessages` import cap across five import add-ons, and two breaking changes affecting Docker add-on availability and OAST/Interactsh compatibility.

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

01 New MCP tools for resource and history access NEW

90

Adds `zap_list_resources`, `zap_read_resource`, and `zap_get_history` tools to the MCP Integration add-on; `zap_get_history` supports body paging via `body_offset` and `max_body_chars` fields.

Use the MCP Integration to page through large HTTP response bodies in history without overwhelming the LLM context window.

```
$ zap_get_history body_offset=0 max_body_chars=2000
```

— Names exact tool and field names with runnable example launch-20260908-0a02c47e

02 maxMessages import limit across import add-ons NEW

80

Adds a `maxMessages` option to the GraphQL Support, Import/Export (HAR), OpenAPI Support, Postman Support, and SOAP Support add-ons to cap the number of messages imported during testing, settable via the UI, the Automation Framework, or the API.

Cap the number of messages imported when pulling in a large OpenAPI spec, to keep scan sessions manageable during auth or access-control testing.

> 📍 In the ZAP OpenAPI Import dialogue, set maxMessages to the desired limit (e.g. 100) before importing — or supply the same field via the Automation Framework job or API call.

— Names exact config key and every affected add-on launch-20260908-0a02c47e

03 AJAX Spider and DOM XSS rule removed from Docker builds

75

BREAKING

The AJAX Spider and DOM XSS Active Scan Rule add-ons are removed from nightly and weekly Docker releases starting the week of 14 September 2026; existing Automation Framework and API jobs continue working, now backed by the Client Spider, while teams must install the add-ons manually from the Marketplace or switch to the Client Spider and OWASP PTK respectively.

— Gives date and clear migration path `launch-20260908-0a02c47e`

04 **LLM Support add-on for chat and MCP integration** NEW

70

New LLM Support add-on (v0.0.1) connects ZAP to Claude (Anthropic), Google Gemini, Azure OpenAI, Ollama, and OpenAI Compatible endpoints, adding a tabbed LLM Chat panel and integrating with the MCP Integration add-on.

— Names providers and version but no config keys `launch-20260908-0a02c47e`

05 **OAST Support drops old Interactsh compatibility** BREAKING

65

OAST Support no longer supports Interactsh servers older than v1.3.0 — interactions are now decrypted using AES-CTR (matching Interactsh server 1.3.0+), and AES-CFB used by older servers is no longer supported.

— Names exact version and encryption change `launch-20260908-0a02c47e`

THINNER COVERAGE BELOW

06 **Send requests on HAR import** NEW

45

Adds an option to send requests when importing a HAR file in the Import/Export add-on, including via the Automation Framework and API.

— Names module and surfaces but no exact flag `launch-20260908-0a02c47e`

07 **Configurable poll verification in authentication** IMPROVED

45

Poll verification in the authentication subsystem now supports a configurable HTTP method and allows existing headers to be overridden.

— Describes change but no exact config field `launch-20260908-0a02c47e`

08 **LLM-driven review and import actions** NEW 40

Adds an LLM-driven Review using LLM/AI action to Alert Filters for re-assessing alert confidence, and an LLM-driven OpenAPI importer to the OpenAPI Support add-on.

— Names two features but no config or mechanism detail launch-20260908-0a02c47e

09 **Network add-on client certificate and background request controls**

NEW 40

Adds an option to support client certificates programmatically in the Network add-on, and an option to control how browser background requests are handled, defaulting to hide.

— Two thin Network add-on options without named flags launch-20260908-0a02c47e

10 **Fuzzer strategies renamed to Cluster Bomb and Pitchfork**

IMPROVED 40

Renames Fuzzer payload replacement strategies in the UI from Depth First and Breadth First to Cluster Bomb and Pitchfork.

— Simple UI rename, no further mechanism launch-20260908-0a02c47e

└──▷ **BREAKING ON UPGRADE**

! The AJAX Spider and DOM XSS Active Scan Rule add-ons are removed from the weekly Docker release starting the week of 14 September 2026; teams that rely on them must install them manually from the Marketplace or switch to the Client Spider and OWASP PTK respectively.

! OAST Support no longer supports Interactsh servers older than v1.3.0 — interactions are now decrypted using AES-CTR (matching Interactsh server 1.3.0+), and AES-CFB used by older servers is no longer supported.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Aviatrix CoPilot

Feedback ⓘ 1 RELEASE · 2026-09-10 NOTES ↗

RANK

Welcome to the comprehensive documentation for Aviatrix's cloud networking platform. Here you'll find everything you need to deploy, configure, and manage your multi-cloud networking infrastructure.

> CoPilot 4.37.0 adds horizontal scaling for Transit Gateways, brings intrusion prevention rule feeds and a new value dashboard to the Distributed Cloud Firewall, and takes Kubernetes onboarding enforcement to general availability, alongside a redesigned VPC/VNet routing view and several smaller networking and UI enhancements.

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

01 **DCF IPS rule feeds and value dashboard** NEW 35

Adds Distributed Cloud Firewall (DCF) IPS Rule Feeds for managing intrusion prevention rule feeds in DCF, and a DCF Value Dashboard for visualizing DCF security value and coverage.

— Two thin DCF additions grouped, no operational detail given

New and Enhanced Features in 4.37.0

02 **Redesigned VPC/VNet routing and route tables** IMPROVED 35

Redesigns VPC/VNet Routing and Private Route Tables for improved network routing visibility and management.

— States purpose but no specifics of what changed New and Enhanced Features in 4.37.0

03 **FireNet decoupled from single gateway** IMPROVED 30

Decouples FireNet from a single gateway, enabling more flexible FireNet deployments.

— Describes architectural change but no deployment steps

New and Enhanced Features in 4.37.0

04 **Gateway start and stop controls** NEW 30

Introduces Gateway Start and Stop controls for managing gateway lifecycle.

— Names control but not exact UI path or command New and Enhanced Features in 4.37.0

05 **Transit Gateway Horizontal Scaling** NEW 25

CoPilot 4.37.0 introduces Transit Gateway Horizontal Scaling for scaling out transit gateway capacity.

— Names capability but no mechanism or config detail New and Enhanced Features in 4.37.0

06 **Certificate Signing Request generation** NEW 25

Adds Certificate Signing Request (CSR) Generation capability within CoPilot.

— Names the capability only, no workflow described New and Enhanced Features in 4.37.0

07 **Packet capture extended to Controller 10.0** IMPROVED 25

Extends Packet Capture availability to Controller 10.0.

— Names version target but no usage detail New and Enhanced Features in 4.37.0

08 **Egress, SNAT, and peering enhancements** IMPROVED 25

Adds Egress, SNAT, and Peering enhancements for more flexible traffic management.

— Vague grouping of enhancements with no specifics New and Enhanced Features in 4.37.0

09 **Kubernetes onboarding enforcement GA** NEW 20

Kubernetes Cluster Onboarding Enforcement on Clouds and DCF on Kubernetes is now generally available.

— GA milestone stated with no usage or config detail New and Enhanced Features in 4.37.0

10 **Improved table views and notifications** IMPROVED 20

Improves Table Views and Notifications for a more actionable operational experience.

— Generic improvement claim, no concrete change named New and Enhanced Features in 4.37.0

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

Vectra AI

Feedback ⓘ 4 RELEASES · 2026-09-10 BLOG ↗ RANK

This is the home page for docs.vectra.ai.

> Vectra AI's v9.14 release rolls out Traffic Visibility Drop Alerting to all customers, expands APIv2.5 with Traffic Lockdown automation, broadens detection coverage for remote-support tools and C2 frameworks, adds Post-Quantum Cryptography visibility to network metadata, and extends deployment support to Proxmox/KVM alongside Microsoft Defender EDR process correlation and wider Microsoft Defender for Endpoint environment coverage.

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

01 **Traffic Visibility Drop Alerting** NEW 75

Adds Traffic Visibility Drop Alerting, now fully available to all customers, delivering health notifications via email, webhook integrations, API, or Syslog when significant drops in observed IPs, traffic bandwidth, or packet volume are detected, using ML-adapted thresholds per customer network.

— Explains delivery channels and thresholds, no config key v9.14 - Observe (2026-09-10)

02 **Microsoft Defender EDR process correlation** NEW 65

Automatically surfaces the probable process behind an NDR detection alongside the detection in the platform and via API, eliminating the need for custom SIEM/SOAR correlation logic.

— Explains mechanism and benefit, no endpoint named v9.14 - Signal (2026-09-10)

THINNER COVERAGE BELOW

03 **APIv2.5 Traffic Lockdown and performance improvements**

IMPROVED 55

APIv2.5 now supports Traffic Lockdown, enabling automation of a broader range of response actions, and gains improved host information retrieval performance in Quadrant UX.

— Names API version and action but no endpoint or flag v9.14 - Control (2026-09-10)

04 **New detections for remote-support tools, C2 frameworks, and web scanning**

NEW 55

Expands Suspect Protocol Activity detections to include Microsoft Quick Assist and Tailscale discovery traffic, identifying potentially unauthorized remote-support and

overlay-network activity, and adds detection coverage for commonly used command-and-control frameworks and web-scanning behavior.

— Names specific tools but C2 frameworks left generic v9.14 - Observe (2026-09-10)

05 **Post-Quantum Cryptography visibility in network metadata** NEW 50

Enhances network metadata with Post-Quantum Cryptography (PQC) visibility, surfacing cryptographic methods used across network communications to help identify where modern and post-quantum cryptography is being adopted.

— Describes capability but no metric or field named v9.14 - Observe (2026-09-10)

06 **Proxmox/KVM deployment support** NEW 45

Supports deploying Brain, Sensor, and Stream on KVM-based environments including Proxmox.

— Names components and platform but no setup steps v9.14 - Platform (2026-09-10)

07 **Microsoft Defender for Endpoint integration expansion** IMPROVED 45

Expands Microsoft Defender for Endpoint integration to Commercial, GCC, GCC High/DoD, and custom Microsoft environments.

— Lists supported environments but no config detail v9.14 - Platform (2026-09-10)

08 **HTTP user agent enrichment for Host ID** IMPROVED 45

Enhances Host ID with observed HTTP user agent information to provide additional context for asset identification and investigation across changing sessions.

— Describes enrichment but no field name or example v9.14 - Signal (2026-09-10)

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Chainguard

Feedback ⓘ 1 RELEASE · 2026-09-11 CHANGELOG ↗ RANK

Chainguard provides trusted open source artifacts for every layer of your modern software stack—containers, language libraries, and VM images.

> Chainguard connected its Libraries to JFrog Catalog for Java (with JavaScript and Python coming by end of September 2026) and shipped a Go 1.27 FIPS base image that lets a single build target different validated crypto modules at deploy time.

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

01 Go 1.27 FIPS image with swappable crypto modules NEW

72

A single Go 1.27 FIPS artifact built from `cgr.dev/chainguard/go-openssl-fips:1.27` can be deployed to environments requiring different validated crypto modules without recompilation at deployment.

Build a single Go 1.27 FIPS artifact and deploy it to environments requiring different validated crypto modules — no recompilation needed at deployment.

```
$ FROM cgr.dev/chainguard/go-openssl-fips:1.27
```

— Gives exact image tag and behaviour; no further mechanism detail

changelog-20260911-d8b66f49

THINNER COVERAGE BELOW

02 Chainguard Libraries in JFrog Catalog NEW

52

Chainguard-built packages can now be pulled through JFrog Catalog, with JFrog Xray scanning and Curation policies continuing to work as before. Java is supported now; JavaScript and Python support is scheduled by end of September 2026.

— Names integration and rollout dates but no config/endpoint to act on

changelog-20260911-d8b66f49

WAS THIS USEFUL? 👍 👎

Google distroless

Feedback ⓘ changes since 2026-08-31

CODE ↗

Language focused docker images, minus the operating system.

└──▷ **GET THIS VERSION**

```
$ git clone --branch commits-2026-08-31
https://github.com/GoogleContainerTools/distroless.git
# already have the repo? check out this version:
$ git checkout commits-2026-08-31
```

└──▷ **BREAKING ON UPGRADE**

! Debian 12 (`debian12`) base image builds are removed — any image pipeline pulling a `debian12` distroless variant will break on upgrade.

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

Prowler

Feedback ⓘ 1 RELEASE · 2026-09-11 NOTES ↗ CODE ↗ RANK

Prowler is the world's most widely used open-source cloud security platform that automates security and compliance across any cloud environment.

> Prowler 5.42.0 adds AWS ISO partition support and configurable Boto3 timeouts for restricted-egress networks, a persistent Trivy vulnerability database cache for air-gapped image scanning, and a compliance catalog integrity test spanning 42 frameworks.

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

01 Configurable AWS Boto3 connect/read timeouts BREAKING

93

Adds `--aws-connect-timeout` and `--aws-read-timeout` CLI flags plus `PROWLER_AWS_BOTO3_CONNECT_TIMEOUT` and `PROWLER_AWS_BOTO3_READ_TIMEOUT` environment variables to control per-call AWS API wait times for restricted-egress networks (VPC endpoints, GovCloud, private deployments). Lowers the default connect timeout from 60s to 10s while keeping the read timeout at 60s, and changes `--aws-retries-max-attempts 0` to disable Boto3 retries entirely (a single attempt) instead of silently falling back to three attempts — automation relying on the old fallback will now only get one attempt.

Scan a GovCloud account from a host that reaches AWS only through VPC endpoints, cutting per-region timeout from ~4 minutes to ~10 seconds per unreachable service.

```
$ prowler aws --region us-gov-west-1 --aws-connect-timeout 10 --aws-read-timeout 60 --aws-retries-max-attempts 0
```

Scan a GovCloud account through VPC endpoints only, cutting per-service timeout from 60 s to 5 s and disabling retries to surface unreachable endpoints quickly.

```
$ prowler aws --region us-gov-west-1 --aws-connect-timeout 5 --aws-read-timeout 60 --aws-retries-max-attempts 0
```

— Names flags, env vars, exact old/new defaults and behaviour change 5.42.0

02 AWS ISO partition and region support NEW

85

Adds support for AWS ISO partitions (`aws-iso` , `aws-iso-b` , `aws-iso-e` , `aws-iso-f`), resolving regions and services from botocore endpoint metadata with no credentials or network access, so ISO regions such as `us-isob-east-1` are accepted by `--region` and `--excluded-region` without a hand-edited `aws_regions_by_service.json` . Adds `PROWLER_AWS_PARTITION` to bootstrap STS calls inside the configured partition's region, preventing routing failures and timeouts in air-gapped deployments such as GovCloud VPC-endpoint-only installs.

Scan an AWS ISO partition region that was previously unsupported without a hand-edited region file.

```
$ prowler aws --region us-isob-east-1
```

Scan an AWS ISO partition region in an air-gapped deployment without editing aws_regions_by_service.json.

```
$ prowler aws --region us-isob-east-1
```

— Names partitions, env var, flags and a concrete region `5.42.0`

---

03 **Persistent Trivy vulnerability database cache** NEW

75

Honors `TRIVY_CACHE_DIR` in the Image provider so Trivy's vulnerability database is downloaded once and reused across scans; pairing it with `TRIVY_SKIP_DB_UPDATE=true` enables scanning images on hosts without internet access.

Scan container images in an air-gapped environment by pointing Prowler at a pre-populated Trivy database and skipping the download.

```
$ export TRIVY_CACHE_DIR=/mnt/trivy-db
export TRIVY_SKIP_DB_UPDATE=true
prowler image myregistry.internal/myapp:latest
```

— Names env vars and gives runnable air-gapped scan pattern `5.42.0`

04 **Compliance catalog integrity test suite** NEW 60

Adds a compliance catalog integrity test that enforces unique requirement IDs, no duplicate check references within a requirement, and that every referenced check exists for its provider, spanning 42 frameworks across AWS, Azure, GCP, GitHub, Kubernetes, and Microsoft 365.

— Describes scope and rules but no user-facing action `5.42.0`

└──▷ **ALSO FROM THESE RELEASES**

. . . .

└──▷ **BREAKING ON UPGRADE**

! `--aws-retries-max-attempts 0` now disables retries entirely (one attempt per call) instead of silently falling back to three; any automation relying on the old silent-fallback behaviour will now make only a single attempt.

! The default Boto3 connect timeout is lowered from 60 seconds to 10 seconds; scans that relied on the longer default to reach slow or high-latency AWS endpoints may now time out where they previously succeeded.

WAS THIS USEFUL? 👍 👎

◆ Runtime Security

Tencent Cloud CubeSandbox

Feedback ⓘ

1 RELEASE · 2026-09-11 NOTES ↗ RANK

Instant, Concurrent, Secure & Lightweight Sandbox for AI Agents.

> CubeSandbox v0.7.1 makes the CubeS3lvol S3 backend opt-in and hardens its cross-node snapshot restore and reclamation, adds external PostgreSQL/MySQL support via `CUBE_DATABASE_DRIVER`, splits template management into a standalone CubeTemplateCenter service, and adds active/standby disaster recovery for CLM alongside virtiofsd hardening.

└──▷ WHAT SHIPPED · 9 FEATURES most completely described first ? what's the number?

01 S3 backend (CubeS3lvol) now opt-in via config BREAKING

90

The CubeS3lvol S3 backend for cross-node pause/resume and snapshots, including on Kubernetes, must now be explicitly enabled via `[cow.s3] enable = true` or the `ONE_CLICK_ENABLE_S3LVOL=1` environment variable; it is disabled by default. Nodes that were relying on it without an explicit setting must add this config after upgrading, or the S3 volume will be disabled.

Opt the S3 backend back in after upgrading a node that previously relied on it without an explicit config.

```ini
[cow.s3]
enable = true
```

— Names exact config key, env var, K8s scope, and breaking upgrade path. v0.7.1

02 Redis database isolation for multi-cluster deployments NEW

81

A new top-level `redis.db` Helm config key applies to CubeMaster, CubeProxy, and CLM, letting multiple CubeSandbox clusters that share one Redis instance isolate logical databases per cluster.

Isolate logical Redis databases per cluster when multiple CubeSandbox clusters share one Redis instance.

```yaml
redis:
  db: 2
```

— Names exact config key and includes an example value. v0.7.1

03 **Batch template deletion via tpl delete** NEW 73

The `tpl delete` subcommand in `cubemastercli` accepts multiple template IDs in a single batch deletion call.

— Names exact subcommand and CLI tool, nothing further given. v0.7.1

04 **Standalone CubeTemplateCenter service** NEW 72

CubeTemplateCenter splits template build, delete, and reclaim operations out of CubeMaster into an independently scalable, multi-replica service, persisting build artifacts to S3/MinIO (AWS S3-compatible storage).

— Explains the architecture split and storage but no config keys given. v0.7.1

05 **External MySQL/PostgreSQL support via CUBE_DATABASE_DRIVER** NEW 70

The `CUBE_DATABASE_DRIVER` variable selects MySQL or PostgreSQL, letting one-click deployments connect to a self-managed external database instance instead of the bundled default.

— Names the exact env var but no further config detail given. v0.7.1

06 **CubeS3lvol snapshot restore and reclamation improvements** IMPROVED 67

Same-bucket cross-node snapshot restore now uses object-storage server-side copy, with added snapshot cancellation and improved delayed-delete reclamation. A still-referenced snapshot can now be deleted immediately, with its underlying storage reclaimed once the last reference is released.

— Details several concrete storage behaviors but no config surface named. v0.7.1

07 **virtiofsd security hardening** IMPROVED 60

virtiofsd now rejects root-directory mutation operations and forged readdirplus requests once a directory whitelist is configured.

— Describes the mechanism but not the whitelist config surface. v0.7.1

THINNER COVERAGE BELOW

08 **Snapshot support for external mount sandboxes** NEW

59

Sandboxes using Host Mount and Volume Plugin external mounts now support snapshot, restore, rollback, and clone operations.

— Lists the operations but no command or endpoint given. v0.7.1

09 **Active/standby disaster recovery for CLM** NEW 35

The lifecycle management service (CLM) now supports active/standby disaster recovery.

— States the capability only, no mechanism or setup detail. v0.7.1

└──▷ **BREAKING ON UPGRADE**

! Nodes that were using the S3 backend without an explicit setting must set `[cow.s3] enable = true` (or `ONE_CLICK_ENABLE_S3LVOL=1`) after upgrading, or the S3 volume will be disabled.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Devicie

Feedback ⓘ 1 RELEASE · SEEN 2026-09-11 PRESS ↗ RANK

Devicie helps IT teams scale secure device management across applications, patching, compliance, and fleet health, with automation built for Microsoft environments.

> Devicie expanded its automated Intune application management to cover 1,500+ Windows and macOS apps, added version rollback, tied app currency to compliance baseline reporting, brought macOS management to parity with Windows in the same portal, and released a free ROI calculator for estimating coverage and time savings.

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

01 **Intune ROI calculator tool** NEW 80

A free browser-based calculator at `https://devicie.com/intune-roi-calculator` lets IT teams compare their organization's Intune application estate against Devicie's managed catalog coverage, with no account or upload required. Users export their application list from the Microsoft Intune admin center, load it into the calculator, and review per-app coverage and estimated annual hours consumed by manual management.

Estimate how much of your Intune application estate Devicie already covers and how many hours per year manual management is consuming — before committing to anything.

📍 In the Microsoft Intune admin center, export your application list, then open `https://devicie.com/intune-roi-calculator` in a browser, load the export, and review per-app coverage and estimated annual hours — no account or upload required.

— Exact URL and runnable step-by-step usage make this fully actionable.

launch-20260911-cb732535

THINNER COVERAGE BELOW

02 **Automated Intune app management for 1,500+ apps** NEW 50

Devicie automatically manages more than 1,500 Windows and macOS applications inside an organization's existing Microsoft Intune tenant, with new versions typically ready within hours of publisher release. This includes line-of-business, internally developed, and complex-installer vendor applications in the same automated pipeline at no additional charge.





— Names scope and speed but no config or command detail. launch-20260911-cb732535

03 **Three-version retention and rollback for apps** NEW

45

Devicie retains the current application version plus the two preceding versions in the tenant, enabling rollback to an earlier release if an update causes problems.

— Clear mechanism stated but no UI or command steps given. launch-20260911-cb732535

04 **macOS app management parity in Intune portal** NEW 45

Enables browsing, configuring, and deploying macOS applications from the same portal and with the same controls as Windows, natively through Intune, removing the need for a separate macOS application management vendor.

— Explains parity and vendor consolidation but no exact steps. launch-20260911-cb732535

05 **App currency reporting alongside compliance baselines** NEW

40

Reports application currency per device from the same system that reports CIS and ACSC Essential Eight baseline compliance for Windows and macOS devices.

— Names compliance frameworks but no path or workflow detail. launch-20260911-cb732535

WAS THIS USEFUL? 👍 👎

Automox

Feedback

1 RELEASE · 2026-09-10

BLOG ↗

RANK

Check out our full list of release notes, and stay up to date with what

> Automox added a way to independently block Policy Execution and Device Scans within Exclusion Windows, backed by API support, new UI indicators, and audit logging.

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

01 Blocked Activities scope for Exclusion Windows NEW

95

Exclusion Windows can now independently suppress Policy Execution, Device Scans, or both, via a new Blocked Activities section on the Exclusion Window configuration page and matching API support for `blocked activities` / scope configuration payload parameters. When a scan is suppressed, the Scan Result Tile shows a Scan Blocked status with a yellow warning shield and tooltip naming the active window, Device Activity Logs record a timestamped entry ('Scan was blocked due to exclusion window: [Window Name]'), the Connection Tile displays a yellow warning icon with Last scan was blocked text, and a warning confirmation modal appears if a manual scan is triggered via `Device Details > Scan` or the bulk `Devices Table > Scan` action while the window is active.

Suppress device scans during a maintenance window without halting policy executions — configure the scope via the Exclusion Window UI.

> 📍 In the Automox Console, open or create an Exclusion Window, locate the Blocked Activities section, check Device Scans only (uncheck Policy Execution), then save the window.

— Names exact API scope params, UI section, and audit log text.

New Exclusion Window Blocked Activities…

WAS THIS USEFUL? 👍 👎

Microsoft Sysinternals

Feedback ⓘ 1 RELEASE · 2026-09-10

BLOG ↗ RANK

Our community is a collaborative place to learn about our products and ask questions! Check out our most popular conversations!

> Microsoft Sysinternals expanded Linux platform coverage with Amazon Linux 2023 support and rewrote ProcDump for Linux in Rust, alongside smaller updates to PipeList and ZoomIt.

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

01 **Amazon Linux 2023 support across Linux tools** NEW 47

Adds Amazon Linux 2023 support across `ProcDump for Linux`, Procmon for Linux, Sysinternals EBPF, and Sysmon for Linux.

— Names four tools and the OS but no mechanism Linux: ProcDump, Procmon, Sysmon; PipeL…

02 **ProcDump for Linux rewritten in Rust** IMPROVED 40

`ProcDump for Linux` 3.5.3 has been rewritten in Rust.

— Names version and language change, no further detail

Linux: ProcDump, Procmon, Sysmon; PipeL…

03 **Long pipe name support in PipeList** IMPROVED 35

`PipeList` v1.03 adds support for long pipe names.

— Names version and capability but no specifics Linux: ProcDump, Procmon, Sysmon; PipeL…

04 **Smooth zooming in ZoomIt** IMPROVED 30

`ZoomIt` v12.22 adds smooth zooming.

— Bare description of a UI behavior change Linux: ProcDump, Procmon, Sysmon; PipeL…

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines

Feedback ⓘ 1 RELEASE · 2026-09-11 CHANGELOG ↗ RANK

Tines lets teams put AI to work across their most sensitive systems, data, and processes, with the security and governance to do it safely.

> Tines shipped case management upgrades—including MCP-based case tools, API case-field updates, change-control comments, priority labels, and audit log retention settings—while also removing an admin API endpoint.

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

01 **Priority labels on cases list** IMPROVED 35

The cases list now shows priority labels for at-a-glance triage.

— Clear UI addition but minimal detail on values changelog-20260911-03d32e8a

02 **API case-field updates** IMPROVED 30

The release adds support for updating case fields via the API, per the 43.2.0 summary.

— No endpoint or field names provided changelog-20260911-03d32e8a

03 **MCP case tools** NEW 25

Tines 43.2.0 adds MCP case tools for working with cases, as noted in the release summary.

— Only named in summary, no further mechanism changelog-20260911-03d32e8a

└──▷ **BREAKING ON UPGRADE**

! Removed endpoint GET `/api`/v1/admin/users/{email}

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Sysinternals Sysmon for Linux

Feedback ⓘ

1 RELEASE · 2026-09-10 NOTES ↗ CODE ↗ RANK

Sysmon for Linux

> Sysmon for Linux 1.5.3 adds ARM64 (aarch64) processor support and extends distribution support to Amazon Linux 2023.

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

01 **ARM64 (aarch64) architecture support** NEW 30

Sysmon for Linux now supports the aarch64 (ARM64) processor architecture, enabling it to run on ARM64-based systems.

— Names the architecture but no install or config detail 1.5.3

02 **Amazon Linux 2023 support** NEW 30

Sysmon for Linux is now available on Amazon Linux 2023 as a supported distribution.

— Names the distribution but no install steps given 1.5.3

WAS THIS USEFUL? 👍 👎

Splunk Security Content

Feedback ⓘ 1 RELEASE · 2026-09-10

NOTES ↗ RANK

Splunk Security Content

> Splunk Security Content v6.6.0 adds 12 new detection analytics spanning browser shells, LOLBAS abuse, macOS AppleScript execution, Socat tunneling, and SCCM abuse, introduces an alpha NIST AI RMF coverage dashboard, and updates 18 existing analytics for improved fidelity.

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

01 **NIST AI RMF coverage dashboard and lookups** NEW 65

Adds the `detection_subcategory_map` and `nist_ai_rmf_subcategories` lookups to support analytic categorization and alignment with the NIST AI Risk Management Framework, and adds an alpha `nist_ai_rmf_control_coverage` dashboard mapping AI-related ESCU detections to the NIST AI RMF Govern, Map, Measure, and Manage functions to help identify coverage gaps.

— Names lookups and dashboard but no usage steps v6.6.0

THINNER COVERAGE BELOW

02 **LOLBAS network connection detections** NEW 50

Adds LOLBAS Network Connection On Uncommon Port to catch rare network activity from trusted system binaries on non-standard ports, and LOLBAS Rare Network Connection to surface anomalous connections from LOLBAS binaries with separate process-group and common-port tuning.

— Names two detections and tuning options, no config detail v6.6.0

03 **Socat network activity detections** NEW 50

Adds Socat Network Listener Binding an Executable and Socat Remote TCP Connection with Local Echo Disabled detections to identify network tunneling, proxying, and C2 activity conducted via Socat.

— Two named detections with purpose, no mechanism detail v6.6.0

04 **macOS AppleScript and osascript detections** NEW 50

Adds MacOS AppleScript Shell Execution and Compilation to improve visibility into script-based execution on macOS, and MacOS Osascript Displaying Suspicious User Prompt to catch deceptive user-interaction attacks via osascript.

— Two named macOS detections, limited mechanism detail v6.6.0

05 **Windows SCCM abuse detections** NEW 50

Adds Windows SCCM Adsource DLL Was Planted In SMS Provider Directory for DLL planting abuse of SCCM components, and Windows SCCM Smsexec Spawned a Suspicious Child Process for abnormal child-process execution from smsexec.

— Two named SCCM detections with brief scope v6.6.0

---

06 **Browser-spawned Unix shell detection** NEW 45

Adds Cisco NVM - Browser Spawned Unix Shell with External Connection detection to identify command execution or C2 activity originating from browsers on Unix endpoints.

— Single named detection, brief purpose only v6.6.0

---

07 **Improved analytics across platforms** IMPROVED 40

Updates 18 analytics across Citrix, Windows, Linux, and macOS environments, improving detection fidelity for Citrix ADC exploitation, pipe-based execution, data destruction, Ghostscript exploitation, PowerShell, event-log manipulation, credential access, and more.

— Broad list of areas improved without specific detection names v6.6.0

---

08 **Builtin account name change detection** NEW 35

Adds Windows Builtin Account Name Was Changed detection to identify account manipulation targeting built-in accounts.

— Bare detection description, no further mechanism v6.6.0

---

09 **Executed browser-copied content detection** NEW 35

Adds 'Windows Content Copied from Browser was Executed' detection to catch suspicious execution workflows involving payloads copied from web content.

— Bare detection description, no further mechanism v6.6.0

---

10 **Linux crontab enumeration detection** NEW 35

Adds Linux Crontab Enumeration detection to identify crontab listing activity used for discovery.

— Bare detection description, no further mechanism v6.6.0

WAS THIS USEFUL? 👍 👎

Tenzir

Feedback ⓘ 1 RELEASE · 2026-09-11 BLOG ↗ RANK

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

> Tenzir added new Microsoft 365, Microsoft Defender, and Azure Log Analytics sources, extended ClickHouse pushdown deep into filters, projections, and nested pipelines, parallelized Kafka and HTTP-based sinks, and gave the sigma operator automatic OCSF matching.

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

01 Microsoft 365 audit log source NEW

95

Adds `from_microsoft_365_activity` operator to collect unified audit records from Microsoft 365, handling Activity API subscriptions, backfills, continuous polling, pagination, retries, and snapshot-backed blob checkpoints; emits original audit fields alongside `microsoft_365_activity` source metadata including `tenant_id`, `content_type`, `content_id`, and `content_created`.

Continuously collect Microsoft 365 general audit events into your pipeline as they become available.

```
$ from_microsoft_365_activity
  auth = {
    tenant_id: secret("m365-tenant-id")
    client_id: secret("m365-client-id")
    client_secret: secret("m365-client-secret")
  }
  content_types = ["Audit.General"]
```

— Full mechanism and runnable example given Tenzir Node v6.17.0: Parallel data move…

02 Automatic OCSF matching in sigma operator IMPROVED

93

The `sigma` operator now performs automatic OCSF matching: it recognizes OCSF-shaped schemas (a string `metadata.version` and an `int64` / `uint64` `class_uid`), covering major SigmaHQ logsources including all Sysmon-backed Windows categories, Linux/macOS process creation, Windows Security/System/PowerShell/Defender channels, Okta, Entra ID, Azure activity logs, AWS CloudTrail, GCP Cloud Audit Logs, and Zeek DNS/HTTP/SMB; use `mapping="direct"` to opt out and match every rule field literally.

Run Sigma rules against OCSF-shaped events from a subscribe source, opting out of structural OCSF recognition to match fields literally instead.

```
$ subscribe "ocsf"
| sigma path="sigma/rules" mapping="direct"
```

— Named flag and example command included `product docs`

---

03 **Predicate and projection pushdown in from_clickhouse** IMPROVED

92

The `from_clickhouse` operator pushes `where` predicates, `select` field selections, and `head` limits down into the SQL `SELECT` sent to ClickHouse, supporting comparisons, `null` checks, `in` with literal lists, and `and` / `or` / `not`, falling back to local evaluation for unsupported types (function calls, `time` / `ip` comparisons, `Enum` / `Decimal` columns). It was then extended to push `time` values against `Date`, `Date32`, `DateTime`, and `DateTime64` columns (including non-UTC time zones), `ip` values and subnet `in` against `IPv4` / `IPv6` columns, equality on enum names, UUIDs, and `FixedString`, ordering on strings, column-to-column comparisons, `starts_with`, `ends_with`, `length_bytes`, substring search, safe arithmetic, and literal expressions, plus field projections of nested fields (e.g. `meta.level`) so only the requested tuple element is fetched, and matching of `ip` literals against String-typed IP columns in table mode. Field projections and row limits are also pushed through branching operators and nested pipelines (`if`, `match`, `fork`, `fork_merge`, `merge`, `parallel`, `group`, `window`, `every`, `load_balance`, `strict`) and through field removal, batching, replacement, history, time shifting, enrichment, and OCSF processing transforms.

— Extensive named mechanism across releases, no runnable example

`Tenzir Node v6.17.0: Parallel data move…`

---

04 **Parallel requests for HTTP sinks** IMPROVED

88

Adds a `parallel` option to `to_splunk`, `to_opensearch`, `to_elasticsearch`, and `to_azure_log_analytics` to send multiple HTTP requests in flight simultaneously, defaulting to the same value now adopted by `to_google_secops`; these four sinks are also made parallelizable so pipelines running with parallelism enabled replicate sink instances across workers.

Increase Splunk HEC throughput by allowing up to 8 in-flight requests per pipeline instance instead of waiting for each response.

```
$ to_splunk "https://splunk.example.org:8088"
  hec_token = secret("hec")
  parallel  = 8
```

— Named flag with runnable example Tenzir Node v6.17.0: Parallel data move…

05 **Microsoft Defender advanced hunting source** NEW 83

Adds `from_microsoft_defender` operator to run arbitrary KQL queries against Microsoft Defender advanced hunting via Microsoft Graph, with app-only Entra authentication and optional `start` / `end` timestamps.

Pull the last 10 device events from Microsoft Defender advanced hunting into a Tenzir pipeline for enrichment or alerting.

```
$ from_microsoft_defender "DeviceEvents | take 10"
  azure_auth = {
    tenant_id: secret("AZURE_TENANT_ID")
    client_id: secret("AZURE_CLIENT_ID")
    client_secret: secret("AZURE_CLIENT_SECRET")
  }
```

— Named operator with runnable example Tenzir Node v6.17.0: Parallel data move…

06 **Azure Log Analytics KQL source (experimental)** NEW 83

Adds `from_azure_log_analytics` operator (experimental) to run KQL queries against Azure Log Analytics workspaces, supporting Entra app-only auth, optional time bounds, configurable query timeouts, and access to Microsoft Sentinel tables.

Query a day of Windows Security Events from an Azure Log Analytics / Sentinel workspace for offline analysis.

```
$ from_azure_log_analytics "SecurityEvent | project
TimeGenerated, Computer, EventID"
  workspace_id = secret("azure-workspace-id")
  azure_auth = {
    tenant_id: secret("azure-tenant-id")
    client_id: secret("azure-client-id")
    client_secret: secret("azure-client-secret")
  }
  start = 2026-01-01
  end   = 2026-01-02
```

— Named operator with runnable example Tenzir Node v6.17.0: Parallel data move…

07 **Parallelized Kafka source and sink** IMPROVED 68

Parallelizes `from_kafka` and `to_kafka` when the pipeline is parallelized, while keeping sequential behavior for `from_kafka` with `count`, non-`stored` `offset`, or `group.instance.id` set, and for `to_kafka` with `key`.

— Named exception conditions but no example `Tenzir Node v6.17.0: Parallel data move…`

WAS THIS USEFUL? 👍 👎

◆ SIEM

Databricks

Feedback ⓘ 9 RELEASES · 2026-09-09 → 2026-09-10 BLOG ↗

RANK

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

> Databricks shipped GA releases for the Excel Add-in and Databricks-managed MCP connectors for Genie One, added maintenance-window scheduling for continuous Lakeflow pipelines, raised Genie Agents' data-source and conversation limits, previewed External Secrets in Unity Catalog and three new Lakeflow Connect connectors, and rolled out a wide set of dashboard, Ask Genie, and Genie One improvements including backend steering, memory confirmation prompts, and relationship-scoped filters.

└──▷ **WHAT SHIPPED · 14 FEATURES** most completely described first ? what's the number?

01 **Maintenance windows for continuous Lakeflow pipelines** NEW

90

Continuous Lakeflow pipelines now support maintenance window scheduling: you specify a day of the week, start hour, and time zone, and Databricks confines runtime upgrades and serverless infrastructure restarts to that one-hour window. Configurable via the Jobs UI, the Pipelines UI, or the Jobs REST API.

— Names exact schedule parameters and three configuration surfaces

Maintenance windows for continuous pipe…

02 **Databricks-managed MCP connectors for Genie One (GA)** NEW

78

Databricks-managed MCP connectors for Genie One are now GA for Google Drive, Gmail, Microsoft 365, Atlassian, and Slack. All connector tool calls are governed through Unity Catalog and Unity Gateway, enforcing built-in policies, approval requirements, and usage/audit logging, and require per-user individual authentication with OAuth tokens that are never shared across users.

— Names governance mechanism and five connected apps, no setup steps

Databricks-managed MCP connectors for G…

03 **Dashboard chart, pivot table, and theme enhancements** NEW

75

Dashboard visuals and theming gain several additions: `Include -style` level of detail (LOD) expressions in YAML in the metric view editor; a `Line shape` control on line/area

charts connecting points with `linear`, `smooth`, or `stepped` lines; an `Apply to` setting on the pivot table color scale to paint cell text as well as background; path map support for connecting ordered point sequences from separate longitude/latitude columns or a single point geometry column into GPS-track-style trajectories; and the ability to export a dashboard theme to a JSON file and import a theme JSON file into another dashboard for reuse.

— Names every constituent control and its exact values

Dashboard enhancements (2026-09-10)

---

04 **Ask Genie context and insights on dashboards** IMPROVED

73

Ask Genie on dashboards gains several context and insight features: suggested starter questions are now scoped to the current dashboard page and widget on published dashboards; Key Insights are generated per dashboard page with a `New insights` badge and a live-generating indicator; the Ask Genie input bar shows the selected chart as context so you can ask about a specific chart; Genie Code now prefers governed metric views over ad-hoc SQL datasets and reuses an existing metric view when building a dashboard; and the `/importBI` Genie Code command supports more parameterized calculations when importing Tableau reports.

— Enumerates five distinct Genie-on-dashboard behaviours

Dashboard enhancements (2026-09-10)

---

05 **New Lakeflow Connect connectors: Anaplan, Anysphere, Celigo**

NEW

70

Lakeflow Connect adds three new Beta connectors: Anaplan, which ingests audit trail events and user account records and can be enabled/disabled from the Previews page; Anysphere (Cursor) Organization, which ingests members and groups as daily snapshots and is toggled via Settings > Previews; and Celigo, which ingests integrator.io audit log events.

Enable the Anysphere Organization connector for your workspace so it can begin ingesting Cursor org members and groups daily.

> 📍 In the Databricks workspace, go to Settings › Previews, locate the Anysphere Organization connector, and toggle it on.

— Names each connector and what it ingests, with an enablement path

Anaplan connector (Beta) (2026-09-09) Anysphere Organization connector (Beta)… Celigo connector (Beta) (2026-09-09)

---

06 **Backend steering for in-progress Genie One responses** NEW

70

Genie One supports backend steering: you can send a steering message while a response is still generating (e.g. `Focus only on Q3 data`) to guide the output without waiting for it to finish or restarting the conversation.

Steer a long-running Genie One response mid-flight to refocus the answer without cancelling and restarting.

> 📍 While Genie One is generating a response, type a steering message (e.g. `Focus only on Q3 data`) in the input box and send it — Genie One will incorporate the guidance into the answer still being generated.

— Explains mechanism and gives a concrete steering example

Genie One enhancements (2026-09-10)

---

07 **Memory confirmation prompts in Genie One** NEW 70

Genie One adds memory confirmation prompts (Beta): the assistant detects facts worth remembering, surfaces a suggestion (e.g. 'Remember: your fiscal year starts in February — save this?'), and requires explicit approval, modification, or rejection before saving.

Review and approve a memory suggestion so Genie One retains a key fact for future conversations.

> 📍 After Genie One surfaces a memory prompt (e.g. 'Remember: your fiscal year starts in February — save this?'), choose Approve, modify the text, or Reject before Genie One stores it.

— Full flow described with a worked example Genie One enhancements (2026-09-10)

---

08 **Databricks Excel Add-in reaches GA with Live query mode** NEW 70

The Databricks Excel Add-in is now GA, connecting Microsoft Excel to a Databricks workspace to browse and import Unity Catalog tables and views, run SQL queries, build pivot tables, use custom functions, and write data back to Unity Catalog. Pivot tables also gain a `Live query` mode that refreshes results in real time as fields are updated.

— Lists full capability set and a named refresh mode

The Databricks Excel Add-in is now gene…

---

09 **External Secrets in Unity Catalog (Beta)** NEW 70

External Secrets in Unity Catalog (Beta) links a Unity Catalog schema to AWS Secrets Manager so its secrets appear as read-only securable objects governed by Unity Catalog privileges, with values read from AWS Secrets Manager on demand.

— Explains the linking mechanism and governance model clearly

External secrets in Unity Catalog (Beta…

10 **Higher Genie Agents data source and conversation limits**

IMPROVED 60

Genie Agents now support up to 50 data sources (tables, views, or metric views) per agent, up from 30, and up to 200,000 stored conversations per agent, up from 10,000.

— Exact before/after numbers but no usage detail Genie Agents enhancements (2026-09-10)

THINNER COVERAGE BELOW

11 **Genie Code skills enabled by default** IMPROVED 55

Genie Code skills are now enabled by default in Genie One, with per-skill toggle controls available on the customization page.

— States default change and a UI toggle location Genie One enhancements (2026-09-10)

12 **Relationship-scoped filters for dashboard widgets** NEW 50

Relationship-scoped filters (Public Preview): on dashboards with defined relationships, each widget now responds only to filters whose dataset is related to it, rather than to every filter on the page.

— Describes new filter scoping behaviour but no config path

Dashboard enhancements (2026-09-10)

13 **SQL warehouse selection for dashboard materialization** NEW 50

When exporting a dashboard dataset as a materialized view in Unity Catalog, you can now choose which SQL warehouse runs the materialization.

— Clear single setting but minimal further detail Dashboard enhancements (2026-09-10)

14 **PowerPoint upload support in Genie One** NEW 35

Genie One conversations now accept direct uploads of `.pptx` (PowerPoint) files.

— Names the format but gives no further mechanism Genie One enhancements (2026-09-10)

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Intruder

Feedback ⓘ changelog · Sep 11, 2026 CHANGELOG ↗

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

Intruder authenticated web scans now support additional domains, subdomains, and cross-domain services in a single scan scope.

└──▷ HOW TO FIND IT

When an app at `app.example.com` relies on `api.example.com` and an external identity provider, add those domains so authenticated scans fully crawl and test all application flows.

📍 In the Intruder console, open the target for your web app, go to Authentication settings, locate the Additional domains field, and add entries such as `api.example.com`, `auth.example.com`, and any external identity provider or CDN URLs your application depends on.

WAS THIS USEFUL? 👍 👎

runZero

Feedback ⓘ 1 RELEASE · 2026-09-11 CHANGELOG ↗ RANK

runZero is a cloud-based asset discovery and inventory platform that continuously identifies and maps all devices and software across networks.

> runZero shipped finer-grained API client permissioning, visibility improvements for gateway-discovered sub-assets, refined hostname discovery logic, and broader cloud asset-type coverage for AWS, Azure and GCP imports.

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

01 **Hostname discovery via WS-Discovery, NetBIOS fallback removed**

55

BREAKING

WS-Discovery `XAddr` endpoints now contribute to asset hostnames, while hostname discovery no longer falls back to NetBIOS domains.

– Clear before/after behaviour change, no migration steps given product docs

02 **Custom-permission API clients with scoped access** NEW

50

API clients can now be created with custom permissions, capped by the creator's own access rights, and account-level API clients support granular authentication scopes.

– Mechanism described but no exact endpoint or flag named changelog-20260911-24eeaafc

03 **Expanded cloud asset matching and types for AWS, Azure, GCP**

IMPROVED

50

Cloud imports now better match directly imported cloud assets, and AWS, Azure, and GCP imports include additional asset types.

– Names three providers but no specific asset types listed product docs

04 **Gateway sub-assets shown in Recent Assets** IMPROVED

35

Sub-assets identified through protocol gateways now appear in the Recent Assets view.

– Brief note naming one UI surface, no further detail changelog-20260911-24eeaafc

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Okta for AI Agents

Feedback ⓘ 1 RELEASE · 2026-09-11

CHANGELOG ↗ RANK

> Okta for AI Agents added IdP-initiated SSO for Square (OIDC), a new Marker.io SCIM integration, and migrated the SAP connector to the SCIM 2.0 API.

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

01 **SAP connector migrated to SCIM 2.0** IMPROVED 55

Migrates the SAP connector to use the SCIM 2.0 API, updating the connector's internal HTTP helper to support the standard.

– Names the API version and internal mechanism changed changelog-20260911-ac92d2d5

02 **IdP-initiated SSO for Square (OIDC)** NEW 40

Enables IdP-initiated SSO flow support for the Square (OIDC) integration, allowing sign-in to be initiated from Okta.

– Names the integration and flow type but no setup steps changelog-20260911-ac92d2d5 changelog-20260911-30b5a1c1

03 **Marker.io by Redblock SCIM integration** NEW 35

Adds Marker.io by Redblock (SCIM) as a new app integration.

– Bare addition, no configuration detail given changelog-20260911-ac92d2d5

WAS THIS USEFUL? 👍 👎

Didit

Feedback

ⓘ

1 RELEASE · 2026-09-11

CHANGELOG ↗

RANK

Didit provides identity verification, fraud prevention, and transaction-monitoring APIs, SDKs, and MCP tools.

> Didit's biggest change this window is per-country control over ID verification methods, anchored by a new non-document lookup path with its own registry-comparison and wallet-credential result blocks, alongside a Web SDK point release.

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

01 **Non-document lookup verification method** NEW 95

Adds non-document lookup as a live verification method — the user submits a national ID number and personal details, which are checked against the authoritative source (government register, credit bureau, or utility/residential records) for that country with no photograph or upload required. Configurable per country via the Countries tab on the ID Verification step or via the API. Includes a configurable retry count (one to five attempts, default two, counting only attempts the source actually answered), format pre-validation so a number that fails the format check never reaches the source and is neither counted nor billed, real-time pricing display in the console for each failure-handling switch before it is saved, and passive liveness plus face-match bundled into the lookup price for countries where the government register returns a portrait (South Africa, Nigeria, Argentina, Panama).

Navigate to the Countries tab in the console to enable non-document lookup for a specific country while keeping document capture as the fallback for failures.

📍 In the Didit console: open your workflow › ID Verification step › Countries tab › select the target country › toggle Non-document lookup ON › set No match and No response failure modes to Document capture › review the per-switch pricing shown › Save.

— Full mechanism, every config option named, with exact console navigation.

changelog-20260911-7d1f33ab

02 **Registry comparison result block in sessions** NEW 60

Adds a Registry comparison result block to sessions, exposing each compared field with the user-provided value, the source-held value, and match status, plus an error row when a source did not respond.

— Names the exact fields shown but gives no navigation or action.

changelog-20260911-7d1f33ab

03 **Web SDK 0.3.1 export and modal fix** IMPROVED 60

Upgrading to `@didit-protocol/sdk-web@latest` (0.3.1) corrects the `SDK_VERSION` export and the viewport-tracking modal, ahead of running an automated integration check.

Upgrade the Web SDK to 0.3.1 to get the corrected `SDK_VERSION` export and viewport-tracking modal before running an automated integration check.

```
$ npm install @didit-protocol/sdk-web@latest
```

— Exact install command and export name given, but little on what was wrong.

changelog-20260911-7d1f33ab

WAS THIS USEFUL? 👍 👎

ConductorOne

Feedback ⓘ 1 RELEASE · 2026-09-11 CHANGELOG ↗

RANK

Govern workforce access, deploy AI agents, and get work done with C1.

> ConductorOne's biggest addition this window is a set of read-only session-policy preview APIs alongside a configurable bulk entitlement request cap, a new Resources tab for governing MCP server resources, stricter SSO authentication handling, and split per-section admin dashboards — plus two breaking changes affecting automation expressions and the Finding API's Owner field.

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

01 **Resources tab for MCP server management** NEW 70

Adds a Resources tab in MCP server management where admins can approve static resources and URI templates discovered on a server; each approved resource gets its own read entitlement governed separately from tool and toolset access.

— Names the tab and governance mechanism; UI path is a clear start.

changelog-20260911-87306871

02 **Stricter compilation for automation expressions** BREAKING 70

Automation expressions that reference the bare workflow context, or pass it to a function, no longer compile — expressions must name the step and field directly. Any automation using an indirect reference will need to be rewritten to a static path before it can be saved again.

— Clear before/after and migration note, no syntax example given.

changelog-20260911-87306871

THINNER COVERAGE BELOW

03 **Strict handling of SSO silent/fresh auth requests** IMPROVED 55

SSO applications now honor OIDC requests for silent or fresh authentication and SAML passive requests; unsafe requests return an error instead of silently reusing an existing session.

— Behavior change explained but no config surface to act on. changelog-20260911-87306871

04 **Per-section admin dashboards** IMPROVED 35

Every admin nav section (except one) now has its own dashboard page, breaking apart what previously lived in a single Product digest view.

— Vague on which sections changed and what dashboards show. changelog-20260911-87306871

└──▷ ALSO FROM THESE RELEASES

.
.
.
.

└──▷ BREAKING ON UPGRADE

! Automation expressions that reference the bare workflow context, or pass it to a function, no longer compile — expressions must name the step and field directly. Any automation using an indirect reference will need to be rewritten to a static path before it can be saved again.

! The `Owner` column, filter, detail field, and corresponding API and webhook field on findings are renamed to `Assignee` — consumers of the Finding object via API, webhook, or audit log (e.g. a SIEM) must update field and event-name references.

WAS THIS USEFUL? 👍 👎

Clerk

Feedback ⓘ 1 RELEASE · 2026-09-11 CHANGELOG ↗ RANK

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

> Clerk added beta support for the OAuth 2.0 Device Authorization Grant, letting browserless devices like CLIs, TVs and game consoles authenticate via a separate browser-capable device.

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

01 **OAuth 2.0 Device Authorization Grant support** NEW 70

Clerk now supports the OAuth 2.0 Device Authorization Grant (RFC 8628) in beta, letting CLIs, TVs, game consoles and other browserless devices obtain tokens by having a user approve access on a separate browser-capable device. It shares Clerk OAuth scopes, tokens, consent context, and Organization claims with the Authorization Code Flow, though PKCE and redirect URIs are not used, and Clerk adds `device_authorization_endpoint` and the `urn:ietf:params:oauth:grant-type:device_code` grant type to its OAuth 2.0 and OpenID Connect metadata when the grant is enabled, enabling automatic discovery.

— Names metadata fields and grant type but no setup steps changelog-20260911-8dea503f

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ 8 RELEASES · 2026-09-11 CHANGELOG ↗ RANK

JumpCloud makes it simple to manage Windows, Apple, Linux, and Android devices and to deliver secure access with SSO, MFA, Zero Trust, RADIUS, and more.

> JumpCloud's biggest window shift was toward identity and AI governance: Password Vault shipped across every surface, Access Risk Detection went GA, and MCP servers in AI Gateway now require SSO-application scoping — alongside new device monitoring, SaaS management, Remote Assist upgrades, and a run of breaking API, LDAP and RBAC changes.

└──▷ **WHAT SHIPPED · 19 FEATURES** most completely described first ? what's the number?

01 Mandatory SSO association for MCP servers BREAKING

88

Existing MCP servers created without an associated SSO application or bookmark must now be assigned one in AI Gateway — access is not scoped by User Groups until an application is assigned, and admins are prompted to assign one on next login. The custom app creation option has been removed from the Add MCP Server dialog; a new application must instead be created via the `+ New App` button, which opens the standard Add New SSO Application wizard, and the new `App` dropdown in Add MCP Server enables user-group-scoped access control.

— Exact dialog names and required migration steps given changelog-20260911-6fcef65f

Release Notes 2026 (2026-09-11)

02 AI agent identity management in AI Gateway NEW

80

Adds `Identity Management > Agents` and `Agent Groups` in the Admin Portal, letting admins register AI agent identities with OAuth client credentials for the JumpCloud AI Gateway, and scope agent access to specific SSO applications via agent groups so it can be audited and revoked independently of human accounts.

Register a new AI agent identity with OAuth credentials so it can access SSO applications independently from employee accounts.

> 📍 In the Admin Portal, go to Identity Management › Agents and click + Add. Fill in the agent name, owner, and company email on the Details tab, then open the Authentication tab and generate OAuth client credentials for the JumpCloud AI Gateway.

Register an AI agent with OAuth credentials and scope its access to specific SSO applications so you can audit and revoke its access independently of human accounts.

📍 In the Admin Portal, go to Identity Management › Agents and click + Add. Fill in the agent name, owner, and company email on the Details tab. Then open the Authentication tab and generate OAuth client credentials for the JumpCloud AI Gateway. Finally, go to Identity Management › Agent Groups, create a group, add the agent, and assign the target SSO applications.

— Exact navigation and OAuth setup steps given via examples `changelog-20260911-6fcef65f` `Release Notes 2026 (2026-09-11)`

---

03 **Escaped pipe character in `$in`/`$nin` filters** IMPROVED

78

Adds support for the pipe `|` character escaped with backslash `\` inside `$in` and `$nin` API filter search terms, e.g. `GET /systemusers?filter=department:$in:Finance \| Accounting|IT`, enabling pipe literals within search values.

Query users whose department is `Finance | Accounting` or `IT`, using the newly escapable pipe character in an `$in` filter.

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

— Exact endpoint and escaped-filter syntax with runnable example

`Release Notes 2024 (2026-09-11)`

---

04 **Password Vault launch across all surfaces** NEW

70

Launches Password Vault across the Admin Portal, User Portal, JumpCloud Protect mobile app, and JumpCloud Go browser extension, enabling secure credential storage, sharing, and autofill with `Connect`, `View Secret`, `View Detail`, `Edit`, and `Manage` permission tiers. Supports bulk import via CSV or Excel, personal and shared folder management, and browser-extension autofill for Non-SSO Website app passwords, 2FA codes, and credential save/update on login and signup.

— Names surfaces and permission tiers but no exact navigation path

`changelog-20260911-6fcef65f` `Release Notes 2026 (2026-09-11)`

---

05 **sso_auth audit event for step-up authentication** NEW

67

Adds a `sso_auth` event to Directory Insights logs for forced re-authentication events (e.g. SP-initiated ForceAuthn requests), giving compliance teams a dedicated audit trail for step-up authentication.

Verify that a high-security app is triggering step-up auth correctly by checking the `sso_auth` event in Directory Insights after a forced re-authentication attempt.

> 📍 In the Admin Portal, go to Directory Insights, filter by event type `sso_auth`, and confirm the event appears with the expected user and timestamp after the SP sent ForceAuthn='true'.

— Named event and log location, verifiable via filter Release Notes 2025 (2026-09-11)

---

06 **Modern TLS cipher enforcement for LDAP** BREAKING 65

Enforces modern TLS cipher suites exclusively for LDAP connections: `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`, `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384`, and `TLS_RSA_WITH_AES_128_GCM_SHA256`.

— Exact cipher list named but no migration guidance given Release Notes 2025 (2026-09-11)

---

07 **Remote Assist remote desktop support** NEW 65

Adds JumpCloud Remote Assist for remote desktop access and support on Windows and macOS devices, installed silently via JumpCloud Agent v1.61.0 or later, with no limits on time or number of sessions. Adds a Ctrl+Alt+Del command shortcut from the Session Options toolbar and user account switching during sessions on Windows devices, plus an inactivity timer.

— Names agent version requirement but no exact session commands

Release Notes 2022 (2026-09-11) Release Notes 2023 (2026-09-11) Release Notes 2024 (2026-09-11)

---

08 **Linux build migrates from AppImage to Debian/RPM** BREAKING 65

Replaces the `.appimage` Linux build of the Password Manager Desktop App with a Debian (Ubuntu x86) build; users must delete their existing `.appimage` build and download the new Debian build. The `.appimage` build is no longer supported as of April 18, 2024, and an RPM build for Red Hat-based distributions is now also offered.

— Exact migration steps and cutover date given Release Notes 2023 (2026-09-11)

What's New: Password Manager Desktop Ap…

---

09 **`$lte`/`$gte` replace `$le`/`$ge` in Dynamic Groups filters** 65

BREAKING

Adds `$lte` and `$gte` operators to Dynamic Groups `memberQuery` filters, replacing the deprecated `$le` and `$ge` operators; existing API calls using `$le` or `$ge` must be updated to the new operator names.

– Exact operator names and migration requirement given Release Notes 2024 (2026-09-11)

10 **Asset Management file uploads and cloning** NEW 60

Adds an Invoice field (File Upload type) to Asset Management so invoices and contracts can be uploaded directly to an asset record, alongside support for custom File Upload fields, and adds asset cloning to streamline creation of assets with shared hardware configurations, with unique fields auto-cleared to prevent duplicates.

– Names field type and behavior, no exact UI path Release Notes 2025 (2026-09-11)

11 **Directory Insights filter refinement** IMPROVED 60

Refines Directory Insights filters by splitting Application Name into Application Name, Application Display Name, and Application Display Label, and Resource Name into Resource Name, Resource Display Name, and Resource Display Label.

– Exact field names given but no workflow guidance Release Notes 2025 (2026-09-11)

THINNER COVERAGE BELOW

12 **SaaS Management and License Management platform** NEW 57

Launches SaaS Management, providing discovery and tracking of SaaS app usage via the JumpCloud Go browser extension, with the ability to categorize, warn on, or block access and track licensing. Releases SaaS License Management generally available, adding connectors for automated license tracking and cost optimization.

– Capability described but no config surface named Release Notes 2024 (2026-09-11) Release Notes 2025 (2026-09-11)

13 **Shadow AI Dashboard** NEW 45

Introduces the Shadow AI Dashboard, a dedicated UI for monitoring generative AI shadow IT with visibility into AI adoption, usage by department, and most active users.

– Describes purpose only, no navigation or config given Release Notes 2025 (2026-09-11)

14 **TOTP MFA for LDAP applications** NEW 45

Adds TOTP as a supported MFA factor for LDAP applications, enabling authentication into LDAP apps via Time-based One-time Passwords in addition to JumpCloud Protect push notifications.

– States capability, no setup steps given Release Notes 2022 (2026-09-11)

15 **MSP billing visibility for committed licenses** NEW

45

Adds billing visibility for MSP customers with committed user licenses, including available/consumed license counts and JumpCloud contract download.

— Describes fields shown but no exact UI path Release Notes 2023 (2026-09-11)

16 **New Android EMM policies** NEW 38

Releases 7 new Android EMM policies for fully managed and dedicated devices, including Factory Reset Protection, Kiosk Mode, and System Updates.

— Names some policies but not all seven or config steps Release Notes 2023 (2026-09-11)

17 **Mac Personalization policy expansion** IMPROVED 37

Expands Mac Personalization policies with updated Dock Settings and Items, and Lock Screen (Screen Saver) policies.

— Bare list of policy names, no mechanism detail Release Notes 2025 (2026-09-11)

18 **JumpCloud Case Portal** NEW 33

Adds JumpCloud Case Portal to centralize support cases and ideas from all administrators in a filterable list with clickable case numbers.

— Bare description, no navigation or filter detail Release Notes 2022 (2026-09-11)

19 **Android 15 full MDM support** NEW 18

Adds Android 15 full MDM support.

— Single bare statement with no scope or mechanism Release Notes 2024 (2026-09-11)

└──▷ **ALSO FROM THESE RELEASES**

Configure a Conditional Access Policy to deny access when disk encryption is off — useful for enforcing encryption compliance across mixed OS fleets.

📍 In the Admin Portal, go to Security › Conditional Access Policies, create or edit a policy, add a Device Condition, and set `disk encryption` to `disabled` with action `Deny`.

Use the Commands feature to install the SentinelOne Agent on all managed Linux devices in one action.

📍 In the Admin Portal, go to Commands, create a new Command, select Linux as the device type, paste the SentinelOne Agent install script, and target the desired device

group.

Create a universal Chrome Browser Patch Management policy to enforce Chrome updates across macOS, Windows, and Linux devices from a single policy.

📍 In the Admin Portal, go to Device Management › Policies, click New Policy, select `Universal Browser Patch Management`, choose Google Chrome, and assign the policy to your device groups.

Set up attribute-based dynamic device group membership to automatically add devices by vendor or public IP address without manual curation.

📍 In Admin Portal, go to Device Groups › select or create a group › enable Dynamic › add a rule using the `Vendor` or `Public IP Address` attribute › save to auto-populate membership.

Monitor upcoming MDM, SSO, and AzureAD token/certificate expirations across all tenants to prevent auth disruptions.

📍 In the Multi-Tenant Portal, go to Home to view the MDM Certificate & Token Status Board showing expiry status for each tenant's MDM, SSO, and AzureAD tokens and certificates.

Enforce MFA for all MSP admins in the tenant from the Multi-Tenant Portal to close gaps where individual admin MFA settings were missed.

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

Connect an AI code editor to JumpCloud via the MCP Server to query org data and automate admin tasks without leaving your development environment.

📍 In the Admin Portal, go to Get Started: JumpCloud MCP Server, generate an MCP Server connection token, then configure your AI tool or code editor to point to the JumpCloud MCP Server endpoint using the generated token.

Enforce conditional access for corporate mobile devices managed by a third-party MDM without migrating MDM providers.

📍 In the Admin Portal, enable Device Trust for third-party managed mobile devices by registering devices via a shared secret and deploying an SSO Extension profile through your existing MDM (Jamf, Kandji, or Google Workspace EMM). Then configure a conditional access policy to restrict protected JumpCloud resources to registered devices only.

└──▷ **BREAKING ON UPGRADE**

! Existing MCP servers created without an associated SSO application or bookmark must now be assigned one in AI Gateway — access is not scoped by User Groups until an application is assigned.

! The custom app creation option has been removed from the Add MCP Server dialog; a new application must be created via the `+ New App` button to open the standard Add New SSO Application wizard before adding a server.

! The `.appimage` Linux build of JumpCloud Password Manager Desktop App is replaced by a Debian (Ubuntu x86) build; users must delete their existing `.appimage` build and download the new Debian build.

! The `GET api/systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; all scripts, automations, or integrations must be updated to use `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body.

! The `$le` and `$ge` filter operators in Dynamic Groups `memberQuery` API requests are deprecated and replaced by `$lte` and `$gte`; existing API calls using `$le` or `$ge` must be updated.

! Existing MCP servers created without an associated SSO application or bookmark must now be assigned one in AI Gateway before access is scoped by User Groups — admins are prompted to assign an application on next login to the AI Gateway console.

! The `Policy Management` scope is renamed to `Access Management`.

! The `System Management` scope is renamed to `Devices`.

! The `Authentication Policies` scope is renamed to `Conditional Access Policies and IP Lists`.

! Identity Management no longer bundles directory and group management — those are now in the separate `Directory and Groups Management` scope, which may break custom roles that relied on the previous bundled structure.

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

WAS THIS USEFUL? 👍 👎

SailPoint

Feedback ⓘ 3 RELEASES · 2026-09-08 → 2026-09-09 BLOG ↗

RANK

SailPoint is an identity and access management platform that automates user provisioning, access governance, and compliance across enterprise systems.

> SailPoint's biggest shift this window is Next-Gen Access Request, a permanent replacement for the legacy Request Center with unified self/other/team/machine-identity requests, enhanced Find Access search, and an AI-driven Harbor Pilot agent; alongside it, Workflows gained a guided Basic mode for trigger filters and File Access Manager 8.5 SP2 added mTLS, Kerberos, and OAuth SMTP authentication support.

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

01 Guided Basic mode for workflow trigger filters NEW

88

Workflow trigger filters gain a Basic mode guided condition builder using AND/OR logic derived from the trigger schema, as an alternative to writing JSONPath expressions; Advanced mode remains available for full JSONPath authoring, including array expressions such as `$.changes[?(@.attribute == 'department')]`. View, Edit, Download, and List operations now present trigger filters in the new format once enabled, and during the Staging-to-Production rollout gap, uploading a workflow JSON in the other environment's filter format will fail — remove the trigger filter, upload, then re-add it in the target environment's UI.

Use the Basic mode filter builder in the Workflows UI to add a trigger filter without writing JSONPath, then verify it matches your test input before promoting.

> 📍 In Identity Security Cloud, go to Workflows › select a workflow with a filterable event trigger › Trigger › Filter › switch to Basic mode › add conditions using AND/OR logic from the trigger schema › save, then open the Test panel and confirm the filter matches your test input.

— Concrete UI steps, exact JSONPath example, and rollout caveat

Enhancement: A Guided Builder for Workf…

02 Enhanced search and discovery in Find Access NEW

73

Find Access adds cross-field catalog search across name, description, source, application, owner, privilege, and access model metadata, with filters for roles, access profiles, entitlements, and applications. Access item cards now show effective privilege labels (HIGH, MEDIUM, or LOW) so requesters can evaluate sensitivity before adding items. When requesting for others, identity search works by name, email, or manager,

with a toggle between All and My Team and support for filtering on up to five public identity attributes configured by an administrator.

– Names filters and labels but no exact UI navigation given

New Capability: Next-Gen Access Request…

03 **Next-Gen Access Request replaces legacy Request Center**

60

BREAKING

SailPoint introduces Next-Gen Access Request, a unified flow for requesting access for self, others, a team, or machine identities, replacing the legacy Request Center. Opting a production tenant into Next-Gen Access Request is permanent and cannot be rolled back; all production tenants will be forcibly migrated on February 16, 2027 if not opted in earlier.

– Names migration deadline but no opt-in steps given

New Capability: Next-Gen Access Request…

04 **New authentication protocols for File Access Manager connectivity**

NEW

60

File Access Manager 8.5 SP2 adds mutual TLS (mTLS) authentication support for NetApp ONTAP connectivity, covering both client-side and server-side authentication; Kerberos authentication support for Microsoft Exchange Server integrations; and OAuth-based SMTP authentication for outbound email, replacing Basic Authentication for Exchange Online compatibility.

– Named integrations and protocols but no config steps given

File Access Manager 8.5 Service Pack 2 …

THINNER COVERAGE BELOW

05 **Harbor Pilot Access Request Agent** NEW

55

For entitled customers, the Harbor Pilot Access Request Agent enables natural-language access request search, interactive selection, form submission, request cancellation with a reason, and request status reporting.

– Lists agent capabilities but no invocation steps given

New Capability: Next-Gen Access Request…

06 **Machine identity request support in Access Request** NEW

40

Next-Gen Access Request adds dedicated machine identity request support for customers with the Machine Identity Security add-on, including filtering by owner or type.

— Names add-on and filters but no further mechanism

New Capability: Next-Gen Access Request…

07 **.NET 10 framework upgrade** IMPROVED 20

File Access Manager's core application framework has been upgraded to .NET 10.

— Bare upgrade note, no impact or migration detail given

File Access Manager 8.5 Service Pack 2 …

└──▷ **BREAKING ON UPGRADE**

! During the Staging-to-Production rollout gap, uploading a workflow JSON that uses the other environment's trigger filter format will fail. Remove the trigger filter from the definition first, then upload the file and re-add the filter in the UI of the target environment. This applies to both JSON and API updates.

! Opting a production tenant into Next-Gen Access Request is permanent — it cannot be rolled back to the legacy Request Center experience. All production tenants are forcibly migrated on February 16, 2027 if not opted in earlier.

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

Firezone

Feedback ⓘ 1 RELEASE · 2026-09-11 BLOG ↗ RANK

Replace your VPN with Firezone, an open-source zero trust access platform built on WireGuard®. Connect users to anything, anywhere.

> Firezone's major addition this window is a full device-trust system layering X.509 certificate-based attestation and mTLS on top of its zero-trust access policies, with broad MDM and PKCS#11/TPM support, plus a minor Android app icon refresh.

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

01 **Device Trust via X.509 certificates and mTLS** NEW 93

Firezone now supports device trust: at connection time the Client presents an X.509 certificate issued by an MDM or enterprise PKI and proves possession of the private key (mTLS) before access is granted. Admins upload issuing CA certificates (PEM or DER) under Settings → Trust Anchors in the admin portal, and add a Require attestation condition to Policies so only Clients with a valid, chained device certificate can reach a protected Resource; Clients can verify their own status under Settings → Device Trust, checking that a certificate is selected, the chain is valid, and the private key is accessible. Device identity is embedded via typed URI SANs — `firezone://serial/<value>`, `firezone://udid/<value>`, `firezone://smbios-uuid/<value>`, `firezone://intune-id/<value>`, `firezone://ws1-uuid/<value>`, `firezone://jamf-id/<value>`, and `firezone://kandji-id/<value>` — or, for a universal/non-MDM path, a certificate with `CN=dev.firezone.device-trust` subject and a `firezone://serial/<serial-number>` URI SAN. Linux supports PKCS#11 providers (including TPM-backed keys, smart cards, HSMs, or software tokens) so keys never leave the device; Windows uses the `LocalMachine\My` store and Windows CNG with optional TPM-backed keys. Certificate revocation is checked via CRL and OCSP, auto-discovered from endpoints advertised in the device certificate, disconnecting and blocking Clients on revocation; when multiple valid certificates exist, the one with the most recent `NotBefore` date is selected to allow seamless renewal. Setup guides are provided for Microsoft Intune (Windows, macOS, iOS/iPadOS, Android), Kandji (Windows, macOS, iOS/iPadOS), and Jamf Pro (macOS, iOS/iPadOS), and the Android app (1.5.14) adds support for this X.509-backed device trust.

Enforce device attestation on a sensitive resource so that only clients presenting a valid MDM-issued certificate can connect.

📍 In the Firezone admin portal: Settings → Trust Anchors → Add Trust Anchor → paste the issuing CA certificate (PEM or DER). Then open the Policy for the

protected Resource, add the `Require attestation` condition, and save.

Provision a TPM-backed device identity on Linux without an MDM, then verify the Client can attest before enforcing the policy broadly.

📍 Issue a certificate with subject `CN=dev.firezone.device-trust` and URI SAN firezone:/ `/serial` /<serial-number>, provision it via a PKCS#11 provider backed by the TPM, configure the Firezone Linux Client to use that PKCS#11 provider, then confirm Settings → Device Trust shows a valid chain and private key access before enabling `Require attestation` in the Policy.

Encode an Intune device ID as a typed URI SAN in a certificate profile so Firezone can use it as the per-device identity claim.

```ini
subjectAltName = URI:firezone://intune-id/00000000-0000-0000-0000-000000000001
```

— Names exact UI paths, config values, URI SAN formats, and revocation mechanism.

Android 1.5.14 (2026-09-11)

THINNER COVERAGE BELOW

02 **Refreshed Android app icon and logos** IMPROVED 10

Updates the Android app icon and other in-app logos to the new `F` mark.

— Cosmetic change with no mechanism or actionable detail. Android 1.5.14 (2026-09-11)

WAS THIS USEFUL? 👍 👎

Zscaler

Feedback ⓘ 1 RELEASE · 2026-09-10 BLOG ↗ RANK

Zscaler is a cloud-based security platform that inspects and filters internet traffic to protect users from threats and enforce policy compliance.

> Zscaler rolled out a modernized GovCloud admin experience built on three new pillars: a unified OneAPI gateway, a consolidated Authentication Service with FIDO2 support, and a single Experience Center console with unified RBAC.

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

01 **Consolidated Authentication Service with FIDO2 enrollment**

NEW 73

Authentication Service is a single OpenID/SAML-based authentication layer for all Zscaler products on GovCloud, replacing per-product IDP federations with a consolidated Federal ICAM integration point. It adds native FIDO2 key enrollment, letting admins enroll FIDO2 keys directly in Zscaler independent of IDP provisioning timelines, and offers a wizard-guided migration to the service with automatic policy carryover and a revert option during the transition window.

— Explains mechanism and migration path but no CLI/API detail 2026-09-10-1e65e8fc

02 **OneAPI unified API gateway** NEW 62

OneAPI is a unified API gateway providing programmatic access to management, configuration, analytics, and event-monitoring capabilities across Zscaler products, enabling integration with CI/CD, SOAR, and SIEM workflows for GovCloud tenants. It is available now for GovCloud Moderate and High tenants with no additional deployment required.

— Names integration surfaces but no endpoints or commands given 2026-09-10-1e65e8fc

THINNER COVERAGE BELOW

03 **Experience Center unified admin console with single RBAC** NEW 57

Experience Center is a unified administration console that consolidates management, configuration, monitoring, reporting, and dashboards across all Zscaler products into a single interface for GovCloud tenants. It also introduces a single RBAC model across all Zscaler products within Experience Center, replacing separate per-product permission systems.

— Describes scope and RBAC change but only as a UI console 2026-09-10-1e65e8fc

WAS THIS USEFUL?  

◆ Data Security & DLP

Cyera

Feedback ⓘ 2 RELEASES · 2026-09-03 → 2026-09-09 BLOG ↗ RANK

Cyera is an AI-native data security platform that helps enterprises discover, classify, govern, and protect sensitive data across cloud, SaaS, on-prem, and AI environments.

> Cyera extended its Agent Guardian to inspect and block sensitive prompts sent to Claude via Anthropic's new inference hooks, and added non-human identity (NHI) management as a new Cyera Identity pillar through its acquisition of Oasis Security.

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

01 **Claude inference hooks in Agent Guardian** NEW 85

Cyera Agent Guardian now integrates with Anthropic's Claude inference hooks to intercept every prompt sent to Claude Chat, Claude Cowork, Claude Code, and Claude Design, allowing or denying it before the model runs. Rollout controls include shadow mode (verdicts logged without blocking), percentage-based rollout for policy tuning, and role-based exclusions, plus configurable failure handling to set whether a timeout blocks or allows through per part of the environment. Verdicts return within Anthropic's five-second default window, grounded in Cyera's pre-classified data inventory (sensitivity, lineage, ownership), and blocked prompts surface in the Agent Guardian alerts view alongside existing PII data leakage policy violations with a reason shown to the end user.

— Names hooks, apps, rollout modes, timing window, but no config keys/commands

launch-20260909-85fc1330

THINNER COVERAGE BELOW

02 **Cyera Identity: non-human identity management** NEW 48

Via the acquisition of Oasis Security, Cyera adds non-human identity (NHI) management to its platform as a new Cyera Identity pillar, enabling continuous, policy-driven control over which workloads and AI agents can access which systems, in what context, and for how long. Cyera Identity connects NHI governance directly to Cyera's data intelligence layer so data access and identity are governed together in a single platform.

— Describes capability and rationale but no concrete surfaces or setup steps

launch-20260903-3a655234

WAS THIS USEFUL? 👍 👎

GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

RegScale

Feedback ⓘ 1 RELEASE · 2026-09-10 BLOG ↗ RANK

RegScale is a compliance automation platform that helps organizations manage security controls, risk assessments, and regulatory compliance requirements.

> RegScale's CLI 6.45.8 release adds a configuration option letting JCAM imports auto-create missing system roles.

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

01 **Auto-create system roles in JCAM imports** NEW 75

A new `jcamSystemRoles` key in `init.yaml` lets you declare system roles that JCAM imports should create automatically when a plan is missing them, along with the five values RegScale requires that JCAM does not send. Omitting the key preserves existing behaviour.

— Names exact config key and file, but not the five required values

CLI 6.45.8 (2026-09-10)

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 11, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue