THE CYBER TOOLCHAIN

NO. 070

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 10, 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 269 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 54 tools

▾ // THE BRIEF

HIDE SAME ISSUE, SAME PROMPT, TWO WRITERS: Opus 5 | GPT-5.5

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. GitHub can now hold a pull request unmergeable while a secret scanning alert is open, so a leaked

vim ? help

credential blocks the merge instead of trailing it. Rapid7 InsightVM asks authenticated hosts for their own open ports rather than scanning for them. Elastic replaced an 88-line DLL search-order hijacking rule with a single field.

PROTECT

Stop a leaked secret from reaching main

GitHub's new ruleset rule blocks merging while secret scanning alerts remain open, turning secret detection from a notification into a gate you cannot ignore. GitGuardian's AI agents triage and deep-analyze every public GitHub and Docker Hub incident with verdicts and risk scores in the incident view, which is the part of public-exposure monitoring that normally eats an analyst's morning.

GitHub · GitGuardian SaaS

PROTECT

Find what's listening without guessing at it

InsightVM 8.58's credentialed pre-port discovery queries authenticated hosts for their open ports directly, so services on odd ports that a network sweep skips still get assessed, and scans stop burning time probing closed ranges. Intruder's authenticated web scans can now follow the app onto explicitly listed additional in-scope domains, closing the gap where auth flows or APIs live on a second hostname and simply went unscanned.

Rapid7 InsightVM · Intruder

DETECT

Catch Linux fileless execution and cut a rule to one field

Elastic 9.4.0 adds telemetry for `memfd_create` and kernel module loads — the anonymous-memory path attackers use to run payloads that never touch disk — and 9.5.0 collapses an 88-line DLL search-order hijacking rule into a single field, which is a rule that can now actually be reviewed and maintained. Tenzir auto-translates Sigma field paths onto OCSF-normalized telemetry, so a community rule runs against your pipeline without hand-mapping every field.

Elastic Security Labs · Tenzir

Does **Opus 5** read better? 👍 👎

OFFENSIVE SECURITY

◆ Post-Exploitation

InGuardians peirates

Feedback ⓘ 1 RELEASE · 2026-09-10

NOTES ↗ RANK

Peirates - Kubernetes Penetration Testing tool

> Peirates v1.1.32 adds four new container escape techniques plus a scanner that detects which of them are exploitable in a given cluster.

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

01 **Four new container escape techniques and detection scanner**

NEW 75

Adds the `docker-socket-breakout` escape that opens an interactive host-root shell when a Docker-compatible socket is accessible, an escape technique for when the node's root filesystem is mounted into the container, an escape exploiting a writeable `/proc/sys/kernel/core_pattern`, and an escape usable when `CAP_PTRACE` is available and the pod has `hostPID` set to true (amd64 only). A new scanner detects which of these four conditions are present in a pod and alerts accordingly.

— Named mechanisms for each escape but no runnable usage example given. v1.1.32

WAS THIS USEFUL? 👍 👎

◆ Exploitation & C2

BC Security powershell-empire

Feedback ⓘ

1 RELEASE · 2026-09-08 NOTES ↗ RANK

Empire is a post-exploitation and adversary emulation framework that is used to aid Red Teams and Penetration Testers.

> Empire v7.0.2 ships over 30 new BOF modules spanning service enumeration, syscall-based evasion, and Active Directory recon, alongside AES-256-GCM encryption, chunked agent uploads, a persistent chdir task, and a new `ps-empire update` subcommand — plus breaking changes to password hashing, staging keys, and CSPRNG generation that require re-staging agents.

└──▷ **WHAT SHIPPED · 21 FEATURES** most completely described first ? what's the number?

01 **Persistent working-directory change for agents** NEW 88

New `POST /api/v2/agents/{id}/tasks/chdir` endpoint and `TASK_CHDIR` (opcode 44) persistently change an agent's working directory across checkins, supported on PowerShell, Python, and IronPython agents.

— Names endpoint, method, and opcode v7.0.2

02 **Syscall and ETW evasion BOFs** NEW 85

New BOF modules for in-memory evasion: `wdtoggle` patches WDigest/Credential Guard in LSASS to re-enable plaintext credential caching, `etw_patching` patches or reverts `EtwEventWrite` in ntdll to degrade ETW logging, `static_syscalls_dump` dumps a target process's memory via static syscall numbers bypassing ntdll hooks, `static_syscalls_inject` injects shellcode into a remote process via static syscalls, `static_syscalls_apc_spawn` spawns a temporary process and injects shellcode via APC queue using static syscalls, and `syscalls_shellcode_injection` injects shellcode into a remote process via direct syscalls.

— Names six BOFs with distinct evasion mechanisms each v7.0.2

03 **Active Directory reconnaissance BOFs** NEW 85

New BOF modules for AD recon and lateral movement: `nonpaged_ldapsearch` runs synchronous non-paged LDAP queries against a domain controller when paged queries are throttled, `ldapsearch` runs LDAP/LDAPS queries with configurable scope, `reconad` performs ADSI-based AD reconnaissance, `domaininfo` reports AD domain membership and Azure AD join status, `addmachineaccount` adds machine accounts for lateral movement, `lapsdump` dumps LAPS passwords (`ms-Mcs-AdmPwd`) from AD

via LDAP, and `netuserenum` enumerates local or domain user accounts via `NetUserEnum` with a configurable filter.

— Names seven AD BOFs with their query mechanisms v7.0.2

04 **Process, host and registry recon BOFs** NEW 85

New BOF modules for host and process introspection: `psx` lists processes annotated with detected security products, `psm` returns detailed single-process info by PID (loaded modules, TCP connections, RDP sessions), `psk` enumerates loaded kernel modules/drivers annotated with security-product driver detection, `psw` enumerates window titles across running processes, `psc` lists processes with active TCP connections and RDP session details, `findmodule` and `findLoadedModule` find processes with a given DLL loaded, `findprochandle` finds processes holding a handle to a named object, `notepad` enumerates open Notepad/Notepad++ windows and extracts displayed file path or in-memory text, `winver` retrieves Windows version, build number and patch revision, `reg_query` performs in-agent registry queries (key enumeration, value lookup, recursive traversal) locally or remotely, and `smbinfo` retrieves SMB server info via `NetServerGetInfo`.

— Names twelve host recon BOFs with their outputs v7.0.2

05 **Password hashing, staging key and RNG hardening** BREAKING 85

Password hashing switched from bcrypt to PBKDF2-HMAC-SHA256 (600K iterations); existing bcrypt hashes are incompatible, requiring password resets or database recreation, and non-default bcrypt users must be manually reset via `PUT /api/v2/users/{id}/password`. Staging key normalization replaced MD5 with SHA-256, requiring agents staged under the old algorithm to be re-staged. CSPRNG generation replaced Python's `random` with `secrets` on the server and random.SystemRandom() on the agent across listeners, stagers, agents, and utilities, requiring all deployed agents to be re-staged.

— Names algorithms, iteration count, endpoint and re-staging impact v7.0.2

06 **Network share, DNS and service-start BOFs** NEW 82

New BOF modules: `netuse_add`, `netuse_list`, and `netuse_delete` map, enumerate, and disconnect mapped network drives; `nslookup` performs DNS lookups via the Windows DNS client API with optional custom server and record type; `vssenum` enumerates Volume Shadow Copies exposed on a host's SMB share (useful for locating offline SAM/SYSTEM/NTDS hives); and `startwebclient` starts the WebClient service via ETW trigger registration.

— Names six BOFs and their operational purpose v7.0.2

07 **InjectSelf option for AMSI/ETW bypass modules** NEW

80

New `InjectSelf` option (default `true`) on `inject_amsi_bypass` and `inject_etw_bypass` modules; set to `false` to target a remote PID instead of injecting into the agent's own process.

— Names option, default, and modules affected v7.0.2

08 **Windows service control BOFs** NEW 80

New BOF modules query and enumerate Windows services via the Service Control Manager: `sc_enum` bulk-enumerates all services on a local or remote host (config, query, failure, and trigger data), `sc_qc` queries a service's configuration (binary path, start type, account, dependencies), `sc_qdescription` queries a service's description, `sc_qfailure` queries a service's failure actions (restart, run command, reboot), and `sc_qtriggerinfo` queries the trigger events that start or stop a service.

— Names all five BOF modules and their SCM data v7.0.2

09 **Chat message persistence, hook and export** NEW 78

Chat messages are now persisted to a new `chat_messages` table (Alembic migration `0003`); the `chat/history` endpoint returns the most recent 20 messages, a new `AFTER_CHAT_MESSAGE_HOOK` core hook fires with (db, message: ChatMessage) after a message is persisted, and a downloadable `report=chat` export (also included in `report=all`) produces `chatlog.csv`.

— Names table, migration, endpoint, hook signature and export format v7.0.2

10 **Local Starkiller directory config** NEW 75

New `starkiller.directory` config option serves an already-built Starkiller instance instead of cloning it from GitHub at startup, enabling air-gapped and distro-packaged installs.

Serve an already-built Starkiller from a local directory for an air-gapped install, bypassing the GitHub clone step at startup.

```yaml
starkiller:
  directory: /opt/starkiller/dist
```

— Names the config key and provides an example value v7.0.2

11 **Cobalt Strike http-config profile parsing** NEW 73

The listener parser now supports the Cobalt Strike `http-config` block in malleable HTTP profiles, wiring `trust_x_forwarded_for` (default `false`) and `block_useragents` (fnmatch globs).

— Names config block and both fields with defaults v7.0.2

12 **ILRepack dependency merging for C# modules** NEW 72

New `MergeReferences` option in the C# module YAML schema enables ILRepack dependency merging via the Empire Compiler's `--merge-references` flag.

— Names YAML option and compiler flag v7.0.2

13 **AES-256-GCM encryption across the stack** IMPROVED 70

AES-256-GCM is now used server- and agent-side: an `AES256GCM` AEAD class in `encryption.py` on the server, `agent/stagers/common/aesgcm.py` for Python/IronPython stagers, and a .NET 4.x `AesGcmHelper` for PowerShell stagers.

— Names classes and files but no user-facing action v7.0.2

14 **krb_session_key credential type** NEW 70

New `krb_session_key` credential type stores Rubeus session keys as `<keytype>:<base64key>`, captured automatically from both `dump` and `asktgt` / `asktgs` command output.

— Names type, storage format, and capture sources v7.0.2

15 **Inveigh credential parser** NEW 70

New `situational_awareness/host/inveigh` credential parser ingests NetNTLMv1/v2 hashes from task output, tagging machine accounts as `inveigh machine_account`.

— Names module path and tagging behaviour v7.0.2

16 **Situational-awareness host enumeration modules** NEW 69

New situational-awareness modules `powershell/situational_awareness/host/processes`, `.../ipconfig`, `.../route`, `.../dir_list`, and `python/situational_awareness/host/processes` emit JSON output for server-side filtering.

— Names all module paths and output format v7.0.2

17 **Chunked agent file uploads** IMPROVED 65

Agent file uploads are now split into 512KB chunks drip-fed across checkins, removing the previous 1MB upload limit, with backward-compatible protocol detection for agents on older versions.

— Explains mechanism and limit but no invocation shown v7.0.2

18 **Consolidated SafeChecks bypass YAMLs** NEW 64

New `SafeChecksPS` and `SafeChecksPython` bypass YAMLs consolidate common bypass snippets, opted into via a stager's `Bypasses` parameter.

— Names YAML files and the opt-in parameter v7.0.2

19 **format_string override and VALUE_ARRAY token** NEW 61

New per-option `format_string` override and `{{ VALUE_ARRAY }}` template token render PowerShell `[Array]` parameters as double-quoted, comma-joined elements.

— Names override and token but limited scope detail v7.0.2

THINNER COVERAGE BELOW

20 **SharpHound C# module for BloodHound enumeration** NEW 53

New SharpHound C# module enables BloodHound Active Directory enumeration from an agent, using ILRepack assembly merging.

— Names module and merging technique, little other detail v7.0.2

21 **Debian 11 install support removed** BREAKING 35

Debian 11 (bullseye) is no longer a supported install platform; it has been removed from the install script, CI matrix, and docs.

— States the removal but no migration guidance given v7.0.2

└──▷ **BREAKING ON UPGRADE**

! Password hashing switched from bcrypt to PBKDF2-HMAC-SHA256 (600K iterations); existing bcrypt hashes are incompatible — reset passwords or recreate the database. Non-default bcrypt users must be manually reset via `PUT /api/v2/users/{id}/password`.

! Staging key normalization replaced MD5 with SHA-256; agents staged under the old algorithm must be re-staged.

! CSPRNG generation replaced `random` with `secrets` (server) and random.SystemRandom() (agent) across listeners, stagers, agents, and utilities; all deployed agents must be re-staged.

! `./ps-empire update` overwrites the base `config.yaml` on every run — move local customizations to `config.user.yaml` before upgrading.

! Debian 11 (bullseye) is no longer a supported install platform; it has been removed from the install script, CI matrix, and docs.

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

ZeroPath

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

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

> ZeroPath's biggest addition is a remote MCP server that lets AI assistants like Claude, Cursor and Codex work with findings with no install or API key, alongside Microsoft Teams alerts, reusable Assistant skills, a reorganized Scanner and Settings navigation, and a jump in final validation coverage to 1,000 findings per scan — paired with several breaking API and permission changes.

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

01 **Remote MCP server for AI assistants** NEW 93

Adds a remote MCP server at `https://zeropath.com/mcp` — point Claude, Cursor, Codex, or any Streamable HTTP client at it, authenticate via browser, and work with findings with no install and no API key required. Connections are read-only until changes are approved, and administrators can revoke all connections organization-wide.

Connect an AI coding assistant to your ZeroPath findings instantly, without managing API keys.

```
📍 # In Claude, Cursor, Codex, or any Streamable HTTP MCP client, # set the MCP server URL to: https://zeropath.com/mcp # Then authenticate via your browser when prompted.
```

— Names exact URL, auth flow, and permission model changelog-20260910-ed06a3ad

02 **Repository field renamed lastScanFailure** BREAKING 70

On repository objects, `lastScanError` is replaced by `lastScanFailure`; any API client or integration reading `lastScanError` will receive no value and must be updated to read `lastScanFailure`.

— Exact old and new field names, clear migration changelog-20260910-ed06a3ad

03 **Integration and repository connection permissions** BREAKING 65

Connecting an integration now requires the Create Integrations or Create Installations permission; adding a repository by URL requires Create Repositories — existing automations without these grants will be refused.

— Names exact permission strings and refusal impact changelog-20260910-ed06a3ad

04 **Per-repository ticket creation permission** BREAKING

62

Adds Ticket creation as a per-repository permission for Jira and Linear, required for organizations using access control; creating Jira and Linear tickets is now a per-repository permission that must be explicitly granted or ticket creation will be refused.

— Names affected integrations and refusal behavior changelog-20260910-ed06a3ad

THINNER COVERAGE BELOW

05 **Microsoft Teams channel notifications** NEW

55

Paste an incoming webhook from Teams into ZeroPath to receive scan notifications and vulnerability alerts as Adaptive Cards, with no Azure AD app registration required.

— Names mechanism and format but no exact steps changelog-20260910-ed06a3ad

06 **Final validation coverage raised to 1,000 findings** IMPROVED

55

Raises final validation coverage to up to 1,000 findings per scan, up from 50.

— Concrete before/after numbers, no mechanism detail changelog-20260910-ed06a3ad

07 **Security posture endpoint returns optional fields** BREAKING

48

Eleven measurements on the security posture endpoint now return no value where there is nothing to measure; clients that expected a numeric zero must treat these fields as optional.

— Names count of affected fields, no endpoint path changelog-20260910-ed06a3ad

08 **Duplicate detection when adding repositories** NEW

45

Adds a duplicate-detection surface when adding repositories, surfacing likely duplicates from host migrations with a git history probe per match.

— Explains mechanism but not exact UI path changelog-20260910-ed06a3ad

09 **Slack reconnection with named missing scopes** IMPROVED

40

Adds Slack reconnection in place, with missing-permission scopes named explicitly.

— Names the fix but no scopes or steps given changelog-20260910-ed06a3ad

10 **Quarterly period option in dashboard** NEW

30

Adds a quarterly period option to the dashboard, which now covers a full year at a glance.

— Bare description of a small UI addition `changelog-20260910-ed06a3ad`

└──▷ BREAKING ON UPGRADE

- ! On repository objects, `lastScanError` is replaced by `lastScanFailure`; any API client or integration reading `lastScanError` will receive no value and must be updated to read `lastScanFailure`.
- ! On secret findings, the explanation ZeroPath generates for a dismissal is withheld from API responses; only a reviewer's own note is returned.
- ! Eleven measurements on the security posture endpoint now return no value where there is nothing to measure; clients that expected a numeric zero must treat these fields as optional.
- ! Connecting an integration now requires the `Create Integrations` or `Create Installations` permission; adding a repository by URL requires `Create Repositories` — existing automations without these grants will be refused.
- ! Creating Jira and Linear tickets is now a per-repository permission; organizations using access control must explicitly grant it or ticket creation will be refused.

WAS THIS USEFUL? 👍 👎

Semgrep

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

Get started with Semgrep to help you catch, flag, and fix real vulnerabilities before they ship.

> Semgrep rolled out Autofix to all customers, decoupled Supply Chain Autofix from Upgrade Guidance, and added webhook support for incident policies, alongside smaller triage and workflow UI improvements. Homebrew installs on Intel Macs are now unsupported.

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

01 **Autofix enabled for all customers** IMPROVED 58

Autofix is now enabled for all customers, though it remains opt-in per finding. It can be triggered from the finding Details page or through the API.

– Names trigger points but no API detail or limits snapshot-20260910

02 **Supply Chain Autofix decoupled from Upgrade Guidance** IMPROVED 50

Supply Chain Autofix is now independent of Upgrade Guidance — pull requests can be opened even when Upgrade Guidance is disabled or has not run.

– Explains before/after behavior but no exact mechanism snapshot-20260910

03 **Webhook action for incident policies** NEW 37

Incident policies now support adding a webhook as an action, in addition to the existing Slack action.

– States the addition but no config or endpoint details snapshot-20260910

04 **Ignore reason and comment for Agentic Workflows triage** NEW 35

Adds the ability to record an ignore reason and a comment when triaging an Agentic Workflows issue.

– Describes the capability but not where in UI snapshot-20260910

05 **Homebrew installs dropped on Intel Macs** BREAKING 30

Homebrew installs of Semgrep are no longer supported on Intel Macs.

– Clear breaking change but no migration guidance given snapshot-20260910

06 **Persistent workflow jobs filters** IMPROVED 20

Workflow jobs filters now persist across page refreshes and navigation.

— Brief UI tweak with no further detail `snapshot-20260910`

└──▷ **BREAKING ON UPGRADE**

! Homebrew installs of Semgrep are no longer supported on Intel Macs.

WAS THIS USEFUL?  

GitHub

Feedback ⓘ 3 RELEASES · 2026-09-09 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's biggest ship in this window is a new ruleset rule that blocks pull requests from merging while secret scanning alerts remain open, alongside enterprise-managed permission controls for Copilot agent operations and a CodeQL 2.27.0 release adding Linux ARM64 support plus new query coverage for Rust, C/C++, Java/Kotlin, C#, and ASP.NET Core.

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

01 Block merges on unresolved secret scanning alerts NEW

95

Adds the `require_secret_scanning_alert_resolution` rule type (with a `secret_types` parameter) to the REST API and the `REQUIRE_SECRET_SCANNING_ALERT_RESOLUTION` rule type to the GraphQL API, plus a Require secret scanning alerts are resolved ruleset rule under Repository > Rulesets in repository, organization, and enterprise settings. The rule blocks PR merges until all introduced secret alerts are cleared, and the `secret_types` parameter can extend blocking to custom or generic patterns beyond default provider patterns.

Enable the secret scanning alert resolution rule via the UI to protect your default branch without writing any API calls.

> 📍 1. Go to your repository (or organization/enterprise) Settings. 2. Navigate to Repository › Rulesets. 3. Create or edit a ruleset targeting your protected branches. 4. Enable Require secret scanning alerts are resolved. 5. Optionally expand Secret types to include custom or generic patterns. 6. Save the ruleset.

— Names endpoint, field, GraphQL type and exact UI navigation.

Block pull requests with exposed secret…

02 Enterprise managed permissions for Copilot agent operations

NEW

75

Admins can centrally block, require human approval for, or auto-allow shell commands, file reads and edits, and network domains for GitHub Copilot agent operations, enforced across the GitHub Copilot app, GitHub Copilot CLI, and Visual Studio Code Agent Host sessions. Policies support per-team scoping, and managed restrictions override and cannot be weakened by user settings, workspace settings, auto-approval rules, or previously saved approvals.

– Describes scope and override behavior but no exact config path.

Enterprise managed permissions for GitH…

---

03 **Linux ARM64 support and per-platform CLI distribution** 75

BREAKING

Adds native Linux ARM64 support for the CodeQL CLI and bundle via the `linux-arm64` per-platform release assets. The generic multi-platform `codeql.zip` distribution will be removed in a future release — users must switch to the per-platform `.zip` for their platform — and the CLI now emits a warning when run from an all-platforms distribution, which can be suppressed by setting `CODEQL_ALLOW_ALL_PLATFORMS_DIST=true`.

– Names asset, env var, and migration path for the deprecation.

CodeQL 2.27.0 adds support for Linux AR…

---

04 **New security queries for Rust and C/C++ SQL sinks** NEW 70

Adds the `rust/command-line-injection` query to detect uncontrolled command lines in Rust code, and adds `PQexec`, `PQexecParams`, `PQprepare`, `PQsendQuery`, `PQsendQueryParams`, and `PQsendPrepare` as SQL injection sinks for `cpp/sql-injection` and related C/C++ queries.

– Names exact query IDs and sink functions but no run command.

CodeQL 2.27.0 adds support for Linux AR…

---

05 **OData taint tracking for C#** IMPROVED 60

Adds taint tracking support for OData action parameter binding in C#, improving detection for vulnerabilities involving `ODataActionParameters` and entities tracked by `Delta`.

– Names specific types tracked but no usage instructions.

CodeQL 2.27.0 adds support for Linux AR…

THINNER COVERAGE BELOW

---

06 **Micronaut framework modeling for Java/Kotlin** NEW 55

Adds modeling for the Micronaut framework in Java/Kotlin, covering HTTP controllers, WebSocket endpoints, configuration injection, data access, security annotations, and HTTP client sinks.

– Lists coverage areas but no concrete usage step.

CodeQL 2.27.0 adds support for Linux AR…

---

07 **Private registry authentication for code scanning default setup**

NEW 50

Enables GitHub code scanning default setup to authenticate with container registries or the GitHub API using an organization's private registry configurations, supporting custom content from private Git sources and Docker registries.

— Describes capability but no config key or UI path given.

CodeQL 2.27.0 adds support for Linux AR…

---

08 **Improved ASP.NET Core MVC action discovery** IMPROVED

50

Improves ASP.NET Core MVC controller and action discovery to more closely match runtime behavior, covering application parts, endpoint mappings, inherited actions, and exclusions.

— Explains scope of the accuracy fix, no actionable step.

CodeQL 2.27.0 adds support for Linux AR…

---

09 **Stricter author-association checks in Actions queries**

IMPROVED

45

Improves how CodeQL evaluates author-association field checks in GitHub Actions event payloads, treating them as protection only when the relevant field is present — this may surface additional alerts for workflows relying on ineffective checks.

— Explains behavior change and its effect on alerts, no user action.

CodeQL 2.27.0 adds support for Linux AR…

└──▷ **BREAKING ON UPGRADE**

! The generic multi-platform `codeql.zip` CLI distribution will be removed in a future release; users must switch to the per-platform `.zip` for their platform. The CLI now emits a warning when run from an all-platforms distribution.

WAS THIS USEFUL? 👍 👎

GitLab

Feedback

1 RELEASE · 2026-09-10

BLOG ↗

RANK

The intelligent orchestration platform for DevSecOps, enabling teams and agents to ship trusted software at enterprise scale.

> GitLab's H1 2026 co-create update centers on new automation surfaces — a User Applications REST API, W3C Trace Context CI variables, and instance-wide Secret Push Protection enforcement — alongside smaller additions spanning Terraform state APIs, Scala code-graph support, merge trains, container registry metadata, and Markdown PDF export.

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

01 **W3C Trace Context CI/CD variables** NEW 85

Introduces `CI_TRACEPARENT` and `CI_TRACESTATE` predefined CI/CD variables bringing W3C Trace Context into jobs for cross-pipeline and distributed-system trace correlation.

Correlate a CI/CD job's trace with upstream telemetry in a distributed system by forwarding the W3C Trace Context variables to an external observability endpoint.

```
$ curl -X POST https://otel-collector.example.com/v1/traces \
  -H "traceparent: $CI_TRACEPARENT" \
  -H "tracestate: $CI_TRACESTATE" \
  -d '{"job": "'$CI_JOB_ID'"}'
```

— Named variables plus a runnable example command

Co-Create: Building GitLab with our use…

THINNER COVERAGE BELOW

02 **Scala support in GitLab Orbit code graph** NEW 55

Adds Scala language support to GitLab Orbit, enabling code-graph definitions for classes, traits, objects, functions, and values in Scala repositories.

— Names entity types covered but no usage steps Co-Create: Building GitLab with our use…

03 **SCIM token inspection in Token Information API** NEW 50

Adds SCIM token support to the Token Information API, enabling identity and access management systems to inspect SCIM tokens alongside other GitLab tokens.

— Explains purpose but no request example or path

Co-Create: Building GitLab with our use…

04 **Terraform state protection rules REST API** IMPROVED

50

Completes the REST API for Terraform state protection rules, supporting retrieve, create, update, and delete operations programmatically.

— Names full CRUD scope but no endpoint path Co-Create: Building GitLab with our use…

05 **User Applications REST API** NEW

45

Adds a REST API to programmatically create, view, update, and delete user-owned OAuth applications.

— Names the API but no endpoint path or method given

Co-Create: Building GitLab with our use…

06 **Instance-wide Secret Push Protection enforcement** NEW

45

Adds an instance-level enforcement setting for Secret Push Protection, letting administrators mandate the control across all projects on a GitLab instance.

— Describes scope but not the exact setting or path

Co-Create: Building GitLab with our use…

07 **Platform details in container registry image indexes** IMPROVED

45

Adds supported-platform details (operating system and architecture) to container image indexes in the container registry.

— Clear what's added but no API or UI reference Co-Create: Building GitLab with our use…

08 **Configurable merge train pipeline limits** NEW

35

Adds configurable merge train pipeline limits so high-throughput teams can set limits that match their plan and capacity.

— No config key or exact limit values given Co-Create: Building GitLab with our use…

09 **PDF export for Markdown files** NEW

30

Adds a PDF export option for Markdown files.

— Bare description with no detail on scope or mechanism

Co-Create: Building GitLab with our use…

WAS THIS USEFUL?  

◆ Secrets Detection & Management

infisical

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

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

> Infisical v0.165.9 introduces a global command menu for the UI, a new environment variable for controlling server run modes, PKI license gating, and duplicate-sync detection for Daytona.

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

01 **INFISICAL_RUN_MODES environment variable** NEW 65

Introduces the `INFISICAL_RUN_MODES` environment variable to control which operational modes the Infisical server runs in.

— Names exact env var but not the available mode values v0.165.9

THINNER COVERAGE BELOW

02 **Global command menu in UI** NEW 40

Adds a global command menu to the UI for fast keyboard-driven navigation across the platform.

— Describes what it does but no exact keybinding or path v0.165.9

03 **PKI license gating** NEW 35

Adds PKI license gating to enforce feature access based on license tier.

— States purpose but no tier names or gated features v0.165.9

04 **Daytona duplicate-sync detection** NEW 25

Adds duplicate-sync detection for the Daytona integration.

— Only named in summary, no mechanism described v0.165.9

WAS THIS USEFUL? 👍 👎

GitGuardian SaaS

Feedback ⓘ 1 RELEASE · 2026-09-07 BLOG ↗

RANK

GitGuardian SaaS is a cloud-based security platform that detects and prevents secrets leakage in git repositories and source code.

> GitGuardian SaaS added dual AI agents to Public Secrets Monitoring that triage and deep-analyze every public GitHub and Docker Hub incident, surfacing verdicts, risk scores, and reasoning directly in the incident view.

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

01 AI agent triage for Public Secrets Monitoring incidents NEW

77

Adds a triage AI agent and a deep analysis AI agent that run over every public GitHub and Docker Hub incident, returning a company-related verdict (Related , Uncertain , or Unrelated) and an agent-computed risk score. A new Analysis tab in the incident investigation details view shows the triage reasoning, deep-analysis findings, and the timeline of both agent passes. Three pre-configured saved views group incidents into company-related, unclear if company-related, and not company-related queues. Agents Analysis is enabled by default for new Public Secrets Monitoring workspaces, with gradual rollout to existing workspaces; customers can request early access through their Customer Success Manager.

Review the AI-generated reasoning for a public incident before deciding whether to escalate a credential rotation to your engineering team.

> 📍 In the Public Secrets Monitoring incident list, open an incident, then select the Analysis tab to see the triage agent reasoning, the deep analysis verdict (Related / Uncertain / Unrelated), and the agent-computed risk score.

— Names the tab, verdict values and rollout flag but no scoring formula.

launch-20260907-21a60e41

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

ffuf

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

Fast web fuzzer written in Go

> ffuf v2.3.0 adds multi-step request chaining via preflight and postflight requests with variable extraction, and bounds response snapshot sizes to control resource usage during large fuzzing runs.

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

01 **Bounded response snapshot size for `-od`/`-audit-log`**

IMPROVED 70

Bounds the `-od` / `-audit-log` response snapshot and response header size to cap on-disk and in-memory growth during large fuzzing runs.

— Names exact flags affected but no size limit given v2.3.0

THINNER COVERAGE BELOW

02 **Preflight and postflight requests with variable extraction**

NEW 55

Adds preflight and postflight requests with variable extraction, enabling multi-step request chains where values captured from an earlier response can be injected into subsequent fuzz requests.

— Describes mechanism but no exact flags or config shown v2.3.0

WAS THIS USEFUL? 👍 👎

Salt Security

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

Salt Security is the only holistic AI security solution for the entire agentic AI lifecycle, from API discovery to posture management to threat protection.

> Salt Security launched Claude Connect, a new integration that gives continuous read-only visibility into MCP servers connected to Claude Enterprise organizations.

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

01 Claude Connect integration for MCP server visibility NEW

87

Adds the Claude Connect integration in the Salt Data Source Hub, which authenticates to Anthropic's Compliance API using a `read:compliance_activities` `-scoped` Compliance Access Key. It polls the Compliance API Activity Feed at `https://api.anthropic.com/v1/compliance/activities` to continuously inventory organization-managed MCP servers, surfacing each server's name, identity, status (active vs. removed), and lifecycle timestamps into the Salt Agentic inventory, where discovered servers are labeled with source Claude Connect and show first- and last-seen times.

Confirm your Claude organization UUID before entering it into Salt — retrieve it from any Compliance API activity record.

```
$ curl -s "https://api.anthropic.com/v1/compliance/activities?
limit=1" \
  -H "x-api-key: <your-compliance-access-key>"
```

Connect Salt to your Claude Enterprise org so MCP server discovery starts immediately.

> 📍 In the Salt dashboard, go to Data Source Hub › Claude Connect tile. Enter your Compliance Access Key (sk-ant-...), your Organization ID (UUID from the organization_uuid field), and optionally an API Base URL (default: `https://api.anthropic.com`). Click Connect — Salt validates the key and runs an initial discovery scan.

— Names endpoint, key scope, and exact setup steps. launch-20260909-91f454b1

WAS THIS USEFUL? 👍 👎

OWASP ZAP

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

The ZAP by Checkmarx Core project

> ZAP shipped a new LLM Support add-on while retiring the AJAX Spider and DOM XSS add-ons from its nightly and weekly release channels.

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

01 **AJAX Spider and DOM XSS add-ons retired** BREAKING 55

The AJAX Spider and DOM XSS add-ons are no longer available in nightly and weekly releases; workflows depending on either add-on will break on those release channels.

— Names both affected add-ons and impacted channels launch-20260908-cb05e9db

02 **LLM Support add-on** NEW 30

OWASP ZAP added a new LLM Support add-on, officially launched in August 2026.

— Named but no detail on capabilities or usage launch-20260908-cb05e9db

└──▷ **BREAKING ON UPGRADE**

! The AJAX Spider and DOM XSS add-ons are no longer available in nightly and weekly releases; workflows depending on either add-on will break on those release channels.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

ALEAPP

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

Android Logs Events And Protobuf Parser

> ALEAPP v2026.3.3 adds 70+ new app parsers alongside deep Android system artifacts, MMKV decryption support, and a combined SMS/MMS messaging artifact.

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

01 **Combined SMS/MMS Messages artifact** NEW 70

Adds a combined SMS and MMS Messages artifact that merges both transports into one table sorted by date, adding a Message Type column (SMS or MMS) and a Source Table column naming the originating table (`sms` , `spam_sms` , or `pdu`).

— Names exact columns and source tables but no query example. v2026.3.3

02 **MMS Attachments artifact** NEW 70

Adds a new MMS Attachments artifact reporting every part row joined to its message, including unreferenced files under `app_parts` and `parts` , with stored content type, sniffed type, size, and a status column.

— Names tables and fields, no worked example given. v2026.3.3

03 **MMKV decryption support** NEW 70

Adds MMKV decryption support via a vendored `mmkv_parser` , correct varint header handling, and a new MMKV - Recovered Records artifact.

— Names the parser module and new artifact, mechanism described. v2026.3.3

04 **Android system artifact parsers** NEW 65

Adds Android system artifacts covering Android users, ADB authorizations, and telecom phone accounts; install sessions, per-user package state, and per-app SSAID artifacts; Android dropbox, tombstone, and ANR crash record artifacts; and App Ops artifacts covering recent accesses, standby buckets, and permission modes, plus permission subsystem `access.abx` parsing.

— Enumerates many artifact types but no per-field detail for most. v2026.3.3

05 **70+ new app parsers** NEW 65

Adds 70+ new app parsers spanning secure messaging (WeChat, Element X, Silent Phone, Tutanota, Dust), password/security managers (Bitwarden, KeePassDX, Aegis, Magisk), productivity/note apps (Joplin, Tasks.org, Orgzly Revived, ColorNote),

media/streaming (NewPipe, AntennaPod, Snapseed, Musicolet, InShot, VivaVideo), navigation/fitness (Organic Maps, OsmAnd, OpenTracks, Trail Sense, Sleep as Android), and others including GETTR, Xiaohongshu, Houseparty, CCleaner, Aurora Store, Breezy Weather, RedReader, Aves Gallery, Solid Explorer, HERE WeGo, Moovit, QR and Barcode Scanner, MX Player, Nova Launcher, Flipboard, Easy Voice Recorder, and CamScanner.

— Names dozens of apps but no per-app field detail. v2026.3.3

THINNER COVERAGE BELOW

06 **Chromium/Chrome browser artifacts** NEW 55

Adds Chrome sync synced tabs and session devices artifacts, Chromium tab restore files reporting navigation entries, and Chromium browsers' HTTP cache artifacts for Android.

— Names three browser artifact types, no field-level detail. v2026.3.3

07 **ExoPlayer media cache artifacts** NEW 50

Adds ExoPlayer media cache artifacts for Twitter, Snapchat, Instagram, and Reddit.

— Names four apps covered, no field or mechanism detail. v2026.3.3

08 **WeChat message decoding improvements** IMPROVED 50

WeChat messages are now fully human-readable with decoded content and media correctly attached to their parent messages.

— Describes before/after behavior, no field names given. v2026.3.3

09 **Xiaohongshu MMKV data parsing** NEW 45

Adds Xiaohongshu account data, recent chats, and app launches parsed directly from MMKV.

— Lists data types recovered but no field or table names. v2026.3.3

10 **Life360 cache artifacts and chat photos** NEW 45

Adds Life360 API cache artifacts and cached photos on chat messages.

— Describes two additions but no mechanism specifics. v2026.3.3

11 **Discord cache artifacts and attachment rendering** NEW 45

Adds Discord API cache artifacts and renders cached attachments on chats.

— Describes rendering behavior but no field names. v2026.3.3

12 **Nearby Fast Pair artifacts** NEW 25

Adds Nearby Fast Pair and discovered item artifacts.

— Bare mention of new artifact, no fields or mechanism. v2026.3.3

13 **Phone Link linked accounts artifact** NEW 25

Adds a Phone Link linked accounts artifact.

— One-line addition with no further detail. v2026.3.3

14 **Samsung IMS service logs support** NEW 25

Adds Samsung IMS service logs support for Android.

— Bare mention, no fields or examples. v2026.3.3

WAS THIS USEFUL? 👍 👎

◆ Malware Analysis

CAPEv2

Feedback ⓘ changes since 2026-09-09 CODE ↗

Malware Configuration And Payload Extraction

CAPEv2 adds a GCP Pub/Sub diagnostic loop with Cloud Monitoring integration and symlink preservation in NFS report copy.

└──▷ GET THIS VERSION

```
$ git clone --branch commits-2026-09-09
https://github.com/kevoreilly/CAPEv2.git
# already have the repo? check out this version:
$ git checkout commits-2026-09-09
```

Adds `_diagnostic_loop` method to the GCP Pub/Sub service that periodically logs status and queue depth using `google.cloud.monitoring_v3`, with optional `pip install google-cloud-monitoring` for precise counts.

Adds `symlinks=True` to the `shutil.copytree` call in `node_get_report_nfs`, preserving symlinks when copying analysis results from workers over NFS.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Fastly

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

Fastly is a content delivery network and edge computing platform that accelerates web content delivery and provides security services.

> Fastly launched a beta Terraform provider rewritten on the Plugin Framework with auto-managed service resources plus TLS, NGWAF, TSIG, and object storage support, and added Direct Fetch to Object Storage for server-side migrations from S3.

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

01 **Direct Fetch for Object Storage migrations** NEW 96

Adds `fastly-object-storage-source-url` request header support on `PutObject` and `UploadPart` S3 API calls, letting Fastly pull object data directly from a source URL server-side instead of requiring the client to upload a payload (sent with `Content-Length: 0`). Partial range transfers are supported via a standard `Range` header (e.g. `bytes=0-41943039`) on `UploadPart` for multipart uploads from a byte-range, and pre-signed URLs can be passed in the header to migrate private assets without exposing long-term credentials.

Trigger a server-side copy of a single S3 object into Fastly Object Storage without downloading it locally first.

```
$ curl -X PUT 'https://<bucket>.storage.fastly.com/<destination-key>' \
  -H 'Content-Length: 0' \
  -H 'fastly-object-storage-source-url: https://<source-bucket>.s3.amazonaws.com/<source-key>' \
  -H 'Authorization: AWS4-HMAC-SHA256 ...'
```

Fetch a specific byte range from a source URL as one part of a multipart upload, avoiding any local data transfer for large-file migrations.

```
$ curl -X PUT 'https://<bucket>.storage.fastly.com/<destination-key>?partNumber=1&uploadId=<upload-id>' \
  -H 'Content-Length: 0' \
  -H 'fastly-object-storage-source-url: https://<source-bucket>.s3.amazonaws.com/<source-key>' \
  -H 'Range: bytes=0-41943039' \
  -H 'Authorization: AWS4-HMAC-SHA256 ...'
```

— Full mechanism, named header/endpoints, and runnable curl examples.

launch-20260908-e624da4c

02 **Core service building blocks as Terraform resources** NEW

68

Adds Terraform resources for core service building blocks: `domain`, `backend`, `ACL` and ACL entries, `config store` and items, `secret store`, `dictionary items`, `cache settings`, `response object`, `request setting`, `custom dashboard`, `syslog logging`, and DNS zone.

— Long named resource list but no usage or mechanism detail.

Fastly Terraform Provider (beta) 0.1.0 …

03 **TSIG keys, object storage access keys, and Cloudfiles logging** NEW

63

Adds a `fastly_tsig_key` resource and `fastly_tsig_keys` data source for managing TSIG keys, a new resource for managing Fastly object storage access keys, and support for Cloudfiles logging via `logging_cloudfiles`.

— Names resources and config key but gives no usage detail.

Fastly Terraform Provider (beta) 0.1.3 …

THINNER COVERAGE BELOW

04 **Auto-managed service resources in Terraform provider** NEW

58

Introduces `_auto` service resources with provider-managed version lifecycle: the provider auto-clones, validates, and activates the service configuration on every CRUD operation.

— Mechanism described but no exact resource names or config.

Fastly Terraform Provider (beta) 0.1.0 …

05 **Next-Gen WAF resources in Terraform provider** NEW 58

Adds Next-Gen WAF (NGWAF) resources covering account rules, workspaces, workspace rules, thresholds, lists, signals, redactions, alert integrations, and virtual patching.

— Names WAF resource areas but no config keys or examples.

Fastly Terraform Provider (beta) 0.1.0 …

06 **TLS resource management in Terraform provider** NEW

49

Adds TLS resources covering certificates, private keys, mutual authentication, activation, subscriptions, and Platform TLS.

— Names TLS areas but no resource names or mechanism.

Fastly Terraform Provider (beta) 0.1.0 …

WAS THIS USEFUL?  

◆ Network Analysis & Monitoring

Security Onion

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

RANK

Security Onion is a free and open platform for threat hunting, enterprise security monitoring, and log management. It includes our own interfaces for alerting, dashboards, hunting, PCAP, detections, and case management.

> Security Onion 3.3.0 introduces Agent Studio with agentic memory and Onion AI Reports Tools for Pro users, alongside Logstash tuning controls, MoM subgrid roles, ES troubleshooting, and drag-and-drop config ordering.

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

01 **Logstash tuning via SOC configuration** IMPROVED 65

Adds `log.level` and `log.format` tuning for Logstash via SOC configuration, and supports tuning multiple Logstash pipelines in SOC ES.

— Names exact config keys but no full workflow launch-20260908-499764fe

THINNER COVERAGE BELOW

02 **Third-party component version updates** IMPROVED 50

Updates Zeek to `8.0.10`, CyberChef to `11.3.0`, and Telegraf to `1.39.3`.

— Exact versions named but no behavioural change described launch-20260908-499764fe

03 **ES Troubleshoot on Grid Screen** NEW 40

Adds an ES Troubleshoot capability accessible from the Grid Screen.

— Names exact UI location but no further mechanism launch-20260908-499764fe

04 **Drag-and-drop ordering for config lists** IMPROVED 40

Supports drag-and-drop ordering for config lists such as custom queries.

— Names UI interaction and an example target launch-20260908-499764fe

05 **Subgrid roles for Manager of Managers** NEW 30

Adds subgrid roles for Manager of Managers (MoM) grids, a Pro feature.

— Named area but no role details given launch-20260908-499764fe

06 **Agent Studio with agentic memory** NEW 25

A new Agent Studio feature is introduced with agentic memory, available for Pro users.

— Named but no mechanism or usage detail given launch-20260908-499764fe

07 **Onion AI Reports Tools** NEW 25

Adds Onion AI Reports Tools, a Pro feature for generating reports with AI assistance.

— Feature named only, no operational detail launch-20260908-499764fe

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Container & Image Security

Chainguard

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

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

> Chainguard shipped Go 1.27 images with runtime-selectable FIPS crypto modules, integrated Chainguard Libraries into JFrog Catalog for Zero-Touch Remediation, and added 39 new container images including FIPS variants of the Kubeflow Pipelines stack.

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

01 **Go 1.27 images with FIPS module selection** NEW 80

Adds Go 1.27 support across the `go`, `go-fips`, and `go-openssl-fips` container images. The `go-openssl-fips` image now selects its FIPS-validated cryptographic module at deployment rather than at build time, letting a single artifact run with either the OpenSSL FIPS provider or the Go Cryptographic Module without recompilation.

— Names exact images and FIPS mechanism, but no deploy example given

changelog-20260910-41f654e8

02 **Chainguard Libraries in JFrog Catalog** NEW 70

Integrates Chainguard Libraries with JFrog Catalog so joint customers can pull Chainguard-built packages through JFrog Artifact Repository without build errors, and enables JFrog Zero-Touch Remediation with patched Chainguard packages. Java support is live now; JavaScript and Python support are planned by end of September 2026.

— Names integration and rollout timeline but no setup steps changelog-20260910-41f654e8

03 **39 new container images added** NEW 60

Adds 39 new container images including 10 FIPS variants of `kubeflow-pipelines-*` components, plus `dbmate`, `hadolint`, `jruby`, `kserve-huggingfaceserver`, `gubernator`, `fortiotel`, `packer`, `security-profiles-operator`, `aws-lambda-dotnet`, `opentelemetry-go-instrumentation`, `presidio-anonymizer`, `redpanda-console-fips`, and others.

— Lists many concrete image names but no usage guidance changelog-20260910-41f654e8

WAS THIS USEFUL? 👍 👎

Aqua Security Trivy

Feedback ⓘ CVE-2026-55092 CVE ↗

└──▷ GET THIS VERSION

```
$ git clone --branch CVE-2026-55092
https://github.com/aquasecurity/trivy.git
# already have the repo? check out this version:
$ git checkout CVE-2026-55092
```

`CVE-2026-55092`: Path traversal via a crafted vulnerability database or other downloaded artifacts (CVSS 7.5, affects `<0.71.1`)

WAS THIS USEFUL? 👍 👎

◆ CNAPP

Plerion

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

Plerion is a cloud security platform that discovers and manages vulnerabilities and misconfigurations across infrastructure.

> Plerion added Google Cloud workload security scanning, extending vulnerability, SBOM, and secrets detection to Compute Engine, Cloud Run, and Cloud Functions with keyless, in-boundary access.

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

01 GCP workload vulnerability and secret scanning NEW

69

Plerion now scans inside Google Cloud workloads — Compute Engine instances, managed instance groups, and custom images, as well as Cloud Run services and Cloud Functions (1st and 2nd gen) — for vulnerabilities, software bill of materials (SBOM), and secrets. All scans run inside a dedicated scanning project within the customer's own organization to keep data in-boundary, and GCP authentication is keyless via workload identity federation (WIF).

— Names services and WIF mechanism but no config or command shown.

Google Cloud workload security:

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SOAR

Tines

Feedback ⓘ 1 RELEASE · 2026-09-10 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 43.2.0 expands Cases with an API for updating fields and new MCP tools, adds audit log retention configuration, formula support in AI provider URLs, dashboard draft/edit mode, and change control comments.

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

01 **Cases tools in Tines MCP integration** NEW 43

Adds Cases tools to the Tines MCP (Model Context Protocol) integration, extending the set of actions available to MCP-connected AI clients.

— Names the integration but not specific tool names. changelog-20260910-03d32e8a

02 **Formulas in AI provider URLs** NEW 40

Adds support for using formulas in AI provider URLs, allowing dynamic values to be inserted into the URL configured for an AI provider.

— No example formula or config location shown. changelog-20260910-03d32e8a

03 **Dashboard draft and edit mode** NEW 40

Adds a draft and edit mode for dashboards, letting users work on dashboard changes before publishing them.

— Clear UI capability but no exact navigation given. changelog-20260910-03d32e8a

04 **Update case fields via API** NEW 35

Tines now supports updating case fields via the API, letting integrations programmatically modify existing case data rather than only creating cases.

— No endpoint path or field names given. changelog-20260910-03d32e8a

05 **Audit log retention period configuration** NEW 32

Adds the ability to configure the retention period for audit logs.

— No config key or default value specified. changelog-20260910-03d32e8a

06 **Change control comments** NEW 20

Adds the ability to attach comments as part of change control.

— Very thin description, no mechanism or scope. changelog-20260910-03d32e8a

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL?

◆ Endpoint Security (EDR/XDR)

Trend Vision One

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

RANK

Trend Vision One is Trend Micro's cloud-based XDR platform providing unified security visibility and threat detection across endpoints, networks, and cloud environments.

> Trend Vision One adds a Gmail add-in that lets users report suspicious emails and manage quarantine directly from their inbox.

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

01 **Gmail add-in for reporting and quarantine** NEW 50

A new Gmail add-in lets users report suspicious emails for analysis with a single click directly from their inbox, and enables self-service quarantine review and management for Gmail users when a quarantine mailbox is configured, reducing admin overhead.

— Names the surface (Gmail add-in) but no config detail or steps.

Gmail add-in support (2026-09-10)

WAS THIS USEFUL?

Iru

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

Manage devices and everything they touch. See how security, IT, and compliance get easier when unified around devices with Iru.

> Iru brought Windows coverage to Vulnerability Management, matching its existing Mac support with app inventory, CVE tracking, severity-based enforcement, and low-disruption patching in one console.

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

01 **Windows support in Vulnerability Management** NEW 75

Iru Vulnerability Management now covers Windows devices alongside existing Mac coverage. It inventories all installed Windows applications, maps them against the National Vulnerability Database (NVD), and ranks findings by severity with an active-exploitation flag. Each CVE is tracked through statuses — active, remediated, or risk-accepted — with device-level counts for fleet-wide visibility. Administrators can set severity-based remediation controls per CVE tier via Enforce immediately, Enforce on a timeframe, or No action under Vulnerability Management > Enforcement Controls, and patching is non-disruptive: silent installs when possible, with a user-facing countdown to save work if an app is open at the enforcement deadline.

Configure severity-based enforcement so critical CVEs are patched immediately while lower-severity findings follow a grace period — reducing exposure on Windows without disrupting users.

📍 In the Iru console, go to Vulnerability Management › Enforcement Controls, select a CVE severity tier (e.g. Critical), and set the remediation action to Enforce immediately, Enforce on a timeframe, or No action.

— Names console path, CVE statuses, enforcement tiers, and patch mechanism.

launch-20260909-6337a374

WAS THIS USEFUL? 👍 👎

◆ SIEM

Databricks

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

RANK

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

> Databricks is preparing two upcoming changes: horizontal scaling for Apps in compliance security profile workspaces, and Data Classification scanning extended to Unity Catalog views.

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

01 **Horizontal scaling for Databricks Apps** NEW 45

Enables horizontal scaling for Databricks Apps in workspaces with the compliance security profile enabled, running an app across multiple instances behind a single app URL for higher availability and concurrency.

.
.
.

— Explains mechanism but no config or flag named Horizontal scaling for Databricks Apps …

02 **Data Classification scans Unity Catalog views** NEW 45

Data Classification (Beta) now extends sensitive-data scanning to Unity Catalog views in addition to tables, classifying view columns for sensitive data using the same detection engine.

— Names scope and engine reuse but no API or setting

Data Classification will soon scan Unit…

WAS THIS USEFUL? 👍 👎

Elastic Security Labs

Feedback ⓘ

2 RELEASES · 2026-08-28 → 2026-09-01 BLOG ↗ RANK

Power insights and outcomes with The Elasticsearch Platform. See into your data and find answers that matter with enterprise solutions designed to help you accelerate time to insight.

> Elastic Security 9.4.0 added new Linux fileless-execution telemetry for `memfd_create` calls and kernel module loads, plus an open-source FENIX testing framework, while 9.5.0 introduced a single-field DLL search-order hijacking detection that replaces an 88-line rule.

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

01 memfd_create process event telemetry NEW

95

Elastic Defend now records a process event whenever a process calls `memfd_create` on Linux (requires kernel 5.10.16+ for eBPF-based event sourcing), starting in Elastic Security 9.4.0. The event captures the syscall arguments via new fields `process.Ext.memfd.name`, `process.Ext.memfd.flags`, `flag_cloexec`, `flag_allow_seal`, `flag_hugetlb`, `flag_noexec_seal`, and `flag_exec`, enabling hunting for fileless ELF execution chains such as download → memfd_create → exec.

Hunt for memfd-based fileless ELF execution chains — download → memfd_create → exec — by querying the new `process.Ext.memfd` fields in Kibana.

```
$ event.category: process AND process.Ext.memfd.name: * AND NOT process.Ext.memfd.flag_noexec_seal: true
```

— Names every field and gives a runnable hunting query.

Linux Detection Engineering - Fileless …

02 Single-field DLL search-order hijacking detection NEW

95

Elastic Defend 9.5.0 adds `dll.Ext.defense_evasions: "DLL Hijack: Masquerading"` to DLL load events, enriching them when a loaded DLL is not Microsoft-signed and its name matches a cached inventory of Windows and system-library DLLs. This collapses detection logic that previously required ~88 lines covering ~2,600 named libraries, 10 excluded Windows system paths, signature checks, and a drop-to-load time window into a single field match.

Write a detection rule that fires on any DLL search-order hijacking attempt, replacing the previous ~88-line rule with a single field match.

```
$ dll.Ext.defense_evasions: "DLL Hijack: Masquerading"
```

— Exact field, value, and before/after line-count comparison given.

From 88 lines to 1: Detecting DLL hijac…

03 **FENIX open-source fileless execution lab** NEW 90

Elastic released FENIX (Fileless Execution for NIX), an open-source lab framework at `github.com/elastic/FENIX` with a `fenix run <technique>` CLI for reproducing and testing memfd-based fileless execution patterns against Elastic Defend telemetry.

Run a representative fileless memfd_create technique in a lab environment using FENIX to generate Elastic Defend telemetry for detection validation.

```
$ git clone https://github.com/elastic/FENIX.git && cd FENIX
make all
python3 -m venv .venv && source .venv/bin/activate
pip install -e .
export FENIX_BIN_DIR=$PWD/bin
fenix run memfd_create
```

— Includes repo link and full runnable install/run commands.

Linux Detection Engineering - Fileless …

THINNER COVERAGE BELOW

04 **Kernel module load detection via load_module event** NEW 50

Elastic Defend adds a `load_module` event action to process events, reporting `init_module` and `finit_module` `-based` loadable kernel module loads for visibility into fileless kernel module activity.

— Names the event action but gives no query or version-specific mechanism.

Linux Detection Engineering - Fileless …

WAS THIS USEFUL? 👍 👎

Sumo Logic

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

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

> Sumo Logic shipped GA Content and Configuration Management (C3M) APIs that let MSSP parent orgs programmatically distribute Cloud SIEM content to child organizations.

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

01 **C3M APIs for MSSP content distribution** NEW 53

The Content and Configuration Management (C3M) APIs are now generally available, letting MSSP parent org users programmatically push and sync Cloud SIEM rules, rule tuning expressions, Library content, monitors, and source templates across child orgs, replacing manual distribution through the Organizations UI.

— Names covered content types but no endpoint paths or methods given.

Content and Configuration Management AP…

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

MISP

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

MISP (core software) - Open Source Threat Intelligence and Sharing Platform

> MISP v2.5.46 hardens outbound URL handling against SSRF, delivers major query-performance improvements for event reports and sightings, and expands Overmind with new workflows, a first-run tutorial, and visualization options.

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

01 SSRF hardening via UrlEgressValidator and CurlClient NEW

70

Introduces a shared `UrlEgressValidator` that enforces a common outbound URL policy, validating schemes and resolved addresses and blocking loopback, link-local, and private destinations across all remote-resource retrieval paths. Extends `CurlClient` with host pinning, controlled and validated redirects, response size limits, and TLS peer verification enabled by default.

— Names the exact validator and client classes and their new checks. v2.5.46

02 Sightings retrieval batching in fetchAttributes IMPROVED

65

Batches sightings retrieval inside MispAttribute::fetchAttributes() instead of querying per attribute, reducing a 5,000-attribute case from 8.1 seconds / 10,661 queries to 0.149 seconds / 6 queries — more than a 50x improvement.

— Names the exact method and gives precise before/after benchmark. v2.5.46

03 Overmind UI workflow and visualization expansions NEW

65

Expands Overmind event quick-action cards with merge attributes, enrich event, contact reporter, delegate publishing, execute ad-hoc workflows, and recorrelate events operations; adds warning-list filtering in correlation graphs, Galaxy support inside Tag Collections, and the first version of the MISP Tutorial; adds card views for additional indexes, server-specific card views, and multiple cards per row; and adds responsive correlation graph timelines with correlated events collapsed by default.

— Enumerates every named Overmind addition with a clear UI entry point. v2.5.46

THINNER COVERAGE BELOW

04 Event report query performance improvement IMPROVED

55

Reduces event report count queries from one per event to one or two grouped queries per page, delivering roughly 19x to 35x improvements for that operation.

— Concrete before/after numbers but no user-facing action. v2.5.46

05 **Warning-list source refresh** IMPROVED 45

Refreshes `misp-warninglists` with new sources including network and security scanners, Network Telescope-derived scanner ranges, Cortex/Xpanse infrastructure, and Telegram-related infrastructure.

— Names the new warning-list sources but not counts or mechanism. v2.5.46

06 **MITRE ATT&CK galaxy content update** IMPROVED 35

Updates MITRE ATT&CK galaxies in `misp-galaxy` to include Detection Strategies and Analytics concepts alongside refreshed tactics, techniques, and sub-techniques.

— Names new concepts but no mechanism or scope detail. v2.5.46

WAS THIS USEFUL? 👍 👎

OpenCTI

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

Open Cyber Threat Intelligence Platform

> OpenCTI 7.260910.0 focuses on operational visibility, adding ingestion logs across multiple feed types, S3 offload metrics for event streams, and a refreshed design system for the UI.

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

01 **Ingestion logs for RSS, JSON, and stream feeds** NEW 44

Adds ingestion logs for RSS feed ingestion, JSON feed ingestion, and stream feed ingestion, enabling operators to audit and troubleshoot data pulls from each of these feed types.

— Names three feed types but no log format or access path 7.260910.0

02 **S3 offload metrics for event streams** NEW 38

Adds metrics and logging for stream events offloaded to S3, giving operators visibility into event offload activity.

— Names the S3 offload mechanism but lacks specific metric names 7.260910.0

03 **Filigran design system V1 in UI** IMPROVED 32

Integrates the Filigran design system V1 into the UI, introducing updated visual components including a Slider input.

— Names one component but no broader scope detail 7.260910.0

WAS THIS USEFUL? 👍 👎

Recorded Future

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

RANK

Get started with the Recorded Future API. Covers authentication, base URLs, API key setup, and how to integrate threat intelligence into your security workflows.

> Recorded Future launched Digital Risk Protection, a unified workspace bringing five external threat-monitoring surfaces together with configurable alerting and an AI triage agent.

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

01 **Digital Risk Protection unified workspace** NEW 65

Launches Digital Risk Protection, a unified workspace covering five external threat surfaces: Malicious Site Monitoring, Impersonation Monitoring, Code Repository Monitoring, Dark Web Brand Monitoring, and Identity Exposure Monitoring. Includes configurable risk thresholds per use case so teams control which detections escalate to Alerts without losing underlying detection coverage, and one-click takedown coordination available across all five use cases from day one.

.
.
.

— Names all five surfaces and platform controls but no UI path or command.

launch-20260909-ba3a1237

02 **Malicious Site Monitoring for lookalike domains** NEW 65

Flags newly registered lookalike domains and phishing infrastructure within hours of registration, using logo detection and image OCR to catch impersonation beyond keyword matching.

— Concrete detection mechanism and timing named, no config surface.

launch-20260909-ba3a1237

03 **AI Triage Agent for detections** NEW 60

An AI Triage Agent for Malicious Site Monitoring and Dark Web Brand Monitoring automatically evaluates high-interest detections and delivers an explicit verdict with reasoning, surfacing only critical, high-priority Alerts.

— Explains mechanism and scope but no way to configure it described.

launch-20260909-ba3a1237

04 **Identity Exposure Monitoring for credentials** NEW 60

Surfaces compromised employee credentials from active infostealer logs within hours of exfiltration, with VIP monitoring available for executive accounts.

— Names mechanism and timing but no setup steps given. launch-20260909-ba3a1237

THINNER COVERAGE BELOW

05 **Dark Web Brand Monitoring** NEW 45

Surfaces brand mentions, planned attacks, and compromised data across underground forums, marketplaces, and ransomware extortion sites.

— Describes coverage areas but not how detections are delivered. launch-20260909-ba3a1237

06 **Impersonation Monitoring for executives** NEW 40

Detects fake executive profiles and company impersonation accounts across social and professional networking platforms.

— Names scope only, no mechanism or configuration detail. launch-20260909-ba3a1237

07 **Code Repository Monitoring** NEW 40

Continuously scans public repositories for exposed credentials, PII, and source code.

— Basic capability description without mechanism or limits. launch-20260909-ba3a1237

08 **Customer Credential Monitoring add-on** NEW 35

A paid add-on that extends credential exposure visibility to an organization's customer base.

— Names the add-on but gives no operational detail. launch-20260909-ba3a1237

WAS THIS USEFUL?  

◆ Detection Engineering

Tenzir

Feedback ⓘ 2 RELEASES · 2026-09-07 → 2026-09-10 BLOG ↗ RANK

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

> Tenzir's biggest window feature is Sigma rules that auto-match OCSF-normalized telemetry via automatic field-path translation, alongside new Kafka Avro/Schema Registry decoding, Azure Blob Storage workload identity federation, ClickHouse query pushdown, a Microsoft 365 activity source, and on-demand schema loading in the Explorer UI.

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

01 **OCSF-native Sigma rule matching** NEW 98

The `sigma` operator automatically matches conformant OCSF events without any configuration, covering 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. It works by rewriting rule predicates to OCSF field paths (e.g. `Image` → `process.path`, `ParentImage` → `process.parent_process.path`, `CurrentDirectory` → `process.working_directory`) guided by the rule's `logsource`, so stock SigmaHQ rules match normalized telemetry without per-rule field mapping. The new `microsoft::windows::ocsf::normalize` pipeline operator normalizes both Sysmon event 1 and Windows Security event 4688 to OCSF Process Activity events, letting a single Sigma rule fire across both producers.

Detect suspicious PowerShell spawned from script engines across both Sysmon and Windows Security producers using a stock SigmaHQ rule on OCSF-normalized events.

```
$ from_file "windows-events.xml" { read_delimited "</Event>\n",
include_separator = true }
microsoft::windows::ocsf::normalize
sigma path =
"sigma/rules/windows/process_creation/proc_creation_win_powershel
l_script_engine_parent.yml"
```

Replay Windows test-lab captures at 10x speed, normalize to OCSF, and match against a stock non-interactive PowerShell rule to produce Detection Findings continuously.

```
$ demo::windows "xml", speed = 10.0
microsoft::windows::ocsf::normalize raw
sigma path =
"sigma/rules/windows/process_creation/proc_creation_win_powershel
l_non_interactive_execution.yml"
```

— Mechanism, field mappings, and two runnable examples all given.

launch-20260907-d48e8fed

02 **Azure Blob Storage workload identity federation** NEW

95

`from_azure_blob_storage` and `to_azure_blob_storage` gain an `azure_auth` record with a `web_identity` field enabling Entra workload identity federation per-operator, so a single node can authenticate to multiple tenants; `web_identity` accepts `token_endpoint`, `token_file`, or inline `token`. The `token_endpoint.query_params` record lets OIDC audience parameters be passed as structured key-value pairs (percent-encoded automatically) instead of concatenated onto the URL, accepting both `string` and `secret` values. Note: `azure_auth` cannot be combined with `account_key`.

Read Azure Blob Storage across multiple Entra tenants using workload identity federation from GitHub Actions, without pinning the node to a single tenant via environment variables.

```
$ from_azure_blob_storage
"abfss://logs@customer1.dfs.core.windows.net/**.json.gz"
  azure_auth = {
    tenant_id: secret("customer1-entra-tenant")
    client_id: secret("customer1-entra-client")
    web_identity: {
      token_endpoint: {
        url: env("ACTIONS_ID_TOKEN_REQUEST_URL")
        query_params: { "audience": "api://AzureADTokenExchange"
}
        headers: { "Authorization": "Bearer " +
env("ACTIONS_ID_TOKEN_REQUEST_TOKEN") }
        path: ".value"
      }
    }
  }
{ read_json }
```

— Full config fields and constraint named, with runnable example. product docs

03 **On-demand schema loading in Explorer** IMPROVED 71

The Explorer now loads stored schemas on demand: clicking `Load schemas` in `Stored data` retrieves schema names and event counts without loading all schemas upfront, and expanding a schema loads field definitions for all schemas once, caching them until `Refresh` is clicked. A `Retry` option appears when schema loading fails, schema search now matches schema names only (not field contents), and the Explorer opens the `Results` tab by default instead of the stored-data view.

Browse stored schemas without waiting for a full load — pull schema names and event counts on demand, then expand only what you need.

> 📍 In the Explorer, go to Stored data › click `Load schemas` to retrieve schema names and event counts. Expand a schema to load field definitions for all schemas; further expansions reuse cached definitions until you click `Refresh`.

— Exact UI labels and behavior named, with walkthrough example.

Tenzir Platform v1.39.2: On-demand sche…

04 **ClickHouse operator query pushdown** IMPROVED 65

The `from_clickhouse` operator now pushes `where`, `select`, and `head` into the SQL query sent to ClickHouse (as `WHERE`, column selection, and `LIMIT`), so ClickHouse reads and transfers only what the pipeline needs.

— Named operator and SQL clauses, but no runnable example. product docs

THINNER COVERAGE BELOW

05 **Improved node startup diagnostics** IMPROVED 48

Node startup diagnostics now include source file locations and line/column pointers for broken `tenzir.operators` definitions and package pipelines, including call-site attribution when errors originate inside user-defined operators.

— Describes mechanism but offers no command or example. product docs

└──▷ **BREAKING ON UPGRADE**

! The `azure_auth` record cannot be combined with `account_key`.

WAS THIS USEFUL? 👍 👎

◆ Security Data Pipeline

Realm Security

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

RANK

Cut SIEM cost without losing a detection. Realm reduces, enriches, and routes security data with detection-aware proof — live in days, no engineers.

> Realm shipped AI-generated risk assessments for every recommended log reduction rule, plus new safeguards that protect detection-critical fields and retain a full backup of reduced data before it's cut.

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

01 **Reduction Rule Assessments via Clarity AI** NEW 65

Every recommended SIEM log reduction rule now ships with an AI-generated Reduction Rule Assessment split into a Reasoning section explaining why the rule is likely effective and a Considerations section flagging where it may not fit a given environment. Realm's Clarity AI reasons over what each log source actually produces and what each destination needs, tuning assessments to the specific conditions defined in each rule rather than generic category descriptions.

— Explains mechanism and inputs but no config/API surface named

Context-Driven SIEM Log Reduction for S…

THINNER COVERAGE BELOW

02 **Detection Integrity for reduction safety** NEW 58

Detection Integrity maps every candidate log reduction against the detections currently running, protects the specific log fields those detections depend on, and flags any at-risk detection as a finding instead of silently discarding the data it needs.

— Clear mechanism described, no UI path or command given

Context-Driven SIEM Log Reduction for S…

03 **Data Haven immutable log backup** NEW 58

Data Haven retains a complete, immutable copy of all reduced log data with OCSF observables attached, keeping it searchable and re-suppliable to any destination if a reduction rule turns out to have been incorrect.

— Describes retention and format but no retrieval command or limit

Context-Driven SIEM Log Reduction for S…

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

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

runZero is a continuous asset discovery and network intelligence platform that maps and monitors all connected devices and vulnerabilities in real-time.

> runZero added granular authentication scopes for account-level API clients and stopped counting background MCP connections against API usage.

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

01 **Granular auth scopes for API clients** NEW 50

Account-level API clients can now use granular authentication scopes in addition to roles, with permissions capped by the creating user's own access rights.

— Describes behavior and permission capping but no exact API or config names.

changelog-20260910-b61e1ca7

02 **MCP connections excluded from API usage** IMPROVED 35

Background MCP connections no longer count against API usage.

— States the change but no mechanism or limits given. changelog-20260910-b61e1ca7

WAS THIS USEFUL? 👍 👎

Intruder

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

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

> Intruder now lets authenticated web app scans follow the application beyond its primary domain, by explicitly listing additional in-scope domains.

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

01 Additional domains for authenticated web app scans NEW

75

A new Additional domains field in the authentication setup for web app targets lets users add subdomains (e.g. `api.example.com`, `auth.example.com`) and external services such as identity providers, CDNs, or third-party APIs, so authenticated scans traverse the full application flow instead of stopping at the primary domain boundary.

When your web app calls across subdomains (e.g. a front-end on `app.example.com` hitting an API on `api.example.com`), add those domains so authenticated scans traverse the full application flow instead of stopping at the primary domain boundary.

📍 In the target's authentication settings, locate the Additional domains field and add each subdomain or external URL (e.g. `api.example.com`, `auth.example.com`, or your identity provider's domain) to include them in the authenticated scan scope.

— Names exact field and example domains, gives clear UI path changelog-20260910-b40a8ee5

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

Rapid7 InsightVM

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

RANK

Rapid7 InsightVM is a vulnerability management platform that identifies, prioritizes, and remediates security vulnerabilities across IT environments.

> InsightVM 8.58 adds credentialed pre-port discovery, letting the scan engine ask authenticated hosts directly for their open ports instead of relying on a network port scan.

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

01 Credentialed pre-port discovery for port enumeration NEW

78

A per-template checkbox under Asset Discovery (available from version 8.58) lets the scan engine authenticate to a host via SSH (TCP 22), Scan Assistant (TCP 21047), or a direct Windows connection and pull the host's authoritative list of listening TCP and UDP ports, replacing the outbound network port scan wherever authentication succeeds. The engine auto-selects the credential method, preferring Scan Assistant, then SSH, then direct Windows connection, and silently falls back to a standard network port scan for hosts with no matching credential; the setting is also exposed via the REST API as documented in the configuration guide.

Enable pre-port discovery on a single scan template via the InsightVM console to test faster, more complete port enumeration on hardened or rate-limited hosts before rolling it out broadly.

> 📍 In the InsightVM console, open the scan template you want to test, go to Asset Discovery, and enable the Pre-port discovery checkbox. Save the template, then run it against a representative group of hosts and compare port lists and scan times against previous results.

— Names exact ports, methods and fallback order; API mentioned but no endpoint given.

2026-09-09-ca018e45

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Clerk

Feedback ⓘ 1 RELEASE · 2026-09-10 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, enabling authentication flows on devices without browsers.

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

01 **OAuth 2.0 Device Authorization Grant (beta)** NEW 70

Clerk now supports the OAuth 2.0 Device Authorization Grant (beta, RFC 8628) for clients that cannot open a browser — CLIs, TVs, game consoles — enabling device-code polling flows without redirect URIs or PKCE. Both public clients (Client ID only) and confidential clients (Client ID + Client Secret) are supported in this flow.

.
.

— Names spec, client types and flow but no exact API/config surface

changelog-20260910-8dea503f

WAS THIS USEFUL? 👍 👎

JumpCloud

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

> Across five years of cumulative release notes and a cluster of 2026 updates, JumpCloud shipped a Password Vault spanning the Admin Portal, User Portal, mobile app, and browser extension, an Agentic IAM layer with Agent Identities and PAM-governed AI agent access, a growing AI Gateway/MCP ecosystem with discovery and token-cost tracking, and GA launches for Access Requests, Access Risk Detection, and Custom Admin Roles — alongside dozens of smaller additions to RADIUS, MFA, MDM, dynamic groups, asset management, and the Multi-Tenant Portal.

└──▷ **WHAT SHIPPED · 35 FEATURES** most completely described first ? what's the number?

01 **Agent Identities and Agentic IAM governance for AI agents**

NEW 86

Adds Agent Identities (Public Preview) under `Identity Management > Agents` to manage non-human AI agent identities: OAuth client credentials are generated on the agent's `Authentication` tab, SSO application access is assigned via `Identity Management > Agent Groups`, and integration with Amazon Bedrock AgentCore is supported. Every registered agent must have an assigned human owner before it can run, creating an automatic audit trail from creation to retirement, and PAM least-privilege rules can be applied directly to agents, granting temporary access that expires automatically when a task completes. A PAM MCP Server is planned (shipping before end of Q4 2026) to replace shared API keys with a zero-setup PAM agent that locks permissions to isolated agent identities.

Register a non-human AI agent with OAuth credentials and scoped SSO application access to audit and control what resources an AI agent can reach.

> 📍 In the Admin Portal, go to Identity Management › Agents and click + Add. Enter the agent name, owner, and company email on the Details tab. On the Authentication tab, generate OAuth client credentials for the JumpCloud AI Gateway. Then go to Identity Management › Agent Groups, create an Agent Group, add the agent, and assign SSO applications.

Register a new AI agent with OAuth credentials so it can access SSO applications independently of any human account.

> 📍 In the Admin Portal, go to Identity Management › Agents and click + Add. Enter the agent name, owner, and company email on the Details tab, then go to the

Authentication tab and generate OAuth client credentials for the JumpCloud AI Gateway. Next, go to Identity Management › Agent Groups, create an Agent Group, add the agent, and assign SSO applications.

Register and configure an AI agent identity so an autonomous agent can authenticate via OAuth and access only its assigned SSO applications.

> 📍 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. On the Authentication tab, generate OAuth client credentials for the JumpCloud AI Gateway. Then go to Identity Management › Agent Groups, create a group, add the agent, and assign the required SSO applications.

Grant an Amazon Bedrock agent a managed identity so its actions are auditable and policy-controlled in JumpCloud.

> 📍 In the JumpCloud Admin Console, go to Agent Identities › Integrate Agents with Amazon Bedrock AgentCore and complete the integration wizard to assign the agent an identity and place it in an Agent Group.

— Names exact tabs, groups, integration, and governance mechanisms.

`Release Notes 2026 (2026-09-10)` `launch-20260910-918b8bcf` `changelog-20260910-6fcef65f`

---

02 **MCP server discovery and connection management in AI & SaaS Management**

NEW 85

Adds `MCP Discovery` and `Token & Cost Tracking` toggles under `Access > AI & SaaS Management > Settings > Enhanced Discovery Options` to discover MCP servers and track token usage and estimated cost from Cursor, Claude Code, OpenCode, Codex, and VS Code Copilot CLI on managed Windows and macOS devices. Adds a mandatory `App` dropdown when adding a new MCP server in AI Gateway to scope access to a specific SSO application or bookmark, and an `MCP Connection` column in `AI & SaaS Management > Applications` showing `Discovered`, `Connected`, or `Not Available` status per app, with an `Add MCP Server` action and a `View` link. Shadow AI discovery automatically finds hidden MCP setups and routes them through the JumpCloud AI Gateway.

Enable MCP server discovery and AI token cost tracking across managed devices to get visibility into AI tool usage in your environment.

> 📍 In the Admin Portal, go to Access › AI & SaaS Management › Settings. Under Enhanced Discovery Options, enable MCP Discovery and Token & Cost Tracking.

Enable MCP server discovery and AI coding tool token cost tracking for all managed devices in your org.

📍 In the Admin Portal, go to the device management settings. Under Enhanced Discovery Options, enable MCP Discovery and Token & Cost Tracking.

Enable MCP server discovery and AI token cost tracking for managed developer workstations running tools like Cursor or VS Code.

📍 In the Admin Portal, go to Access › AI & SaaS Management › Settings. Under Enhanced Discovery Options, enable MCP Discovery and Token & Cost Tracking.

Review which managed-device apps have discovered MCP servers and connect one to AI Gateway for group-scoped access control.

📍 In the Admin Portal, go to Access › AI & SaaS Management › Applications. Check the MCP Connection column for Discovered status, click the status to review discovered servers, then click Add MCP Server to connect to AI Gateway.

— Names exact settings path, toggle labels, and connection states.

Release Notes 2026 (2026-09-10) launch-20260910-918b8bcf changelog-20260910-6fcef65f

---

03 **Password Manager Desktop App: Linux/ARM builds, capacity, and UI improvements**

IMPROVED 84

Adds Password Manager trial support so admins can explore the feature by adding a user group, and a Linux Desktop App build (Debian/Ubuntu x86) that supports automatic updates, replacing the prior `.appimage` build — which is no longer supported as of April 18, 2024, requiring migration to the RPM or Debian build. Adds an ARM build for macOS M-series (M1+) devices with automatic update to the ARM build, Download Logs and Keyboard Shortcuts options under Settings, multi-select functionality, item sorting including sort by nickname, a Cloud Backup toggle under Password Manager Settings, and scales item storage capacity to up to 13,000 items with autofill enabled or up to 30,000 items without autofill, with a single shared folder supporting up to 5,000 items.

Enable Cloud Backup for JumpCloud Password Manager so users have a secure fallback if their local vault is lost.

📍 In the Admin Portal, go to Password Manager › Settings, locate Cloud Backups, and toggle Enable Cloud Backup on to activate the feature for your organization.

— Names exact builds, settings options, and item-capacity numbers.

What's New: Password Manager Desktop Ap… Release Notes 2024 (2026-09-10) Release Notes 2023 (2026-09-10) Release Notes 2022 (2026-09-10)

---

04 **API filter syntax: pipe escaping and $lte/$gte operators**

82

BREAKING

Enables the pipe `|` character to be escaped with a backslash `\` inside `in` and `nin` API filter search terms, e.g. `GET /systemusers?filter=department:$in:Finance | Accounting|IT`. Replaces the deprecated `$le` and `$ge` Dynamic Groups `memberQuery` filter operators with `$lte` and `$gte` — API integrations using the old operators must be updated.

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%20%7C%20Accounting|IT' -H 'x-api-key: <api_key>'
```

— Gives runnable example queries and exact deprecated/replacement operators.

Release Notes 2024 (2026-09-10)

---

05 **Password Vault across Admin Portal, User Portal, mobile app, and browser extension**

NEW

80

Introduces JumpCloud Password Vault across the Admin Portal, User Portal, JumpCloud Protect mobile app, and JumpCloud Go browser extension. Admins can enable the vault, assign access to users and user groups, and manage shared credentials and folders with `Connect` / `View` / `Edit` / `Manage` permissions, with activity logged to Directory Insights. Users can view and autofill secrets in mobile apps and the mobile browser, bulk-import credentials via CSV or Excel in the User Portal, manage personal and shared folders with `Connect`, `View Secret`, `View Detail`, and `Manage` permissions, and get launch-and-autofill for non-SSO websites, 2FA codes, and password saving via the JumpCloud Go extension without device registration.

— Covers all four surfaces and permission levels named in the release notes.

Release Notes 2026 (2026-09-10) changelog-20260910-6fcef65f

---

06 **AI Gateway proxies AI client traffic with third-party integrations**

NEW

80

Launches JumpCloud MCP Server GA, connecting compatible AI tools and code editors to JumpCloud administrative capabilities via the Model Context Protocol. Adds AI Gateway to proxy and secure AI client traffic, with integrations for `Apollo.io`, `Asana`, `Atlassian Rovo`, `Cloudflare`, `Datadog`, `GitHub`, `GitLab`, `Google Workspace Apps`, `HubSpot`, `JumpCloud MCP Server`, `Linear`, `Slack`, and `Vanta`, and supports

connecting AI clients — ChatGPT, Claude, Copilot CLI, Cursor, Gemini CLI, OpenAI Codex, and VS Code — to the gateway.

Route and authenticate an AI client (e.g. Claude) through the JumpCloud AI Gateway to enforce identity-aware access controls on AI traffic.

> 📍 In the JumpCloud Admin Console, go to AI Gateway › AI Clients, then follow `Users: Connect Claude to the AI Gateway` to configure the gateway endpoint and credentials for the Claude client.

Connect an AI tool or code editor to JumpCloud via the MCP Server to query org data and run administrative actions programmatically.

> 📍 In the Admin Portal, go to Settings › JumpCloud MCP Server and follow the `Get Started: JumpCloud MCP Server` guide to generate credentials and configure your AI tool's MCP endpoint.

— Names every integration and AI client the gateway connects to.

`Release Notes 2025 (2026-09-10)`

---

07 **Dynamic Device and User Groups with attribute-based rules**

NEW 76

Adds Dynamic Device Groups and Dynamic User Groups automation, enabling attribute-based membership rules with optional pre-review of membership changes before they take effect. Adds `Vendor` and `Public IP Address` as new attributes for dynamic device groups, and `Manager` as a new attribute for dynamic user groups.

Set up a dynamic device group that automatically adds devices by vendor and public IP address, eliminating manual group management.

> 📍 In the Admin Portal, go to Device Groups › Create Group, enable Dynamic, add a rule for Vendor equals `Apple`, add a second rule for Public IP Address in your corporate range, and save to activate automatic membership.

— Names every new attribute and shows a working rule configuration.

`Release Notes 2023 (2026-09-10)`

---

08 **MFA and authentication method enhancements in JumpCloud Protect**

IMPROVED 76

Adds Duo Universal Prompt support for JumpCloud MFA ahead of Duo's March 30, 2024 end-of-support for the traditional prompt; splits WebAuthn enrollment into separate `Security Keys` and `Device credentials` credential types for admins and users; enables MFA by default for all new admin accounts, requiring a second factor at Admin Portal login (with an org-wide `Global MFA Requirement` toggle under Account > Settings); adds

JumpCloud Protect push notification recovery to fetch missed notifications without requiring the user to re-send; and adds Push Bombing Mitigation settings under Security > MFA Configurations to tune or disable the lockout window after repeated push attempts.

Enable Push Bombing Mitigation settings for your org to tune the 60-second lockout window — or disable it for high-volume scenarios — via MFA Configurations in the Admin Portal.

> 📍 In the Admin Portal, go to Security › MFA Configurations, locate the JumpCloud Protect Push Bombing Mitigation section, and set the maximum concurrent attempts or toggle the feature off.

Enforce MFA across all MSP admins in a tenant from the Multi-Tenant Portal without touching individual admin accounts.

> 📍 In the Admin Portal, go to Account › Settings and enable `Global MFA Requirement`.

— Names every distinct MFA change and gives exact settings locations.

`Release Notes 2023 (2026-09-10)`

---

09 **AI & SaaS Management shadow IT and AI app discovery** IMPROVED

73

Renames JumpCloud SaaS Management to JumpCloud AI & SaaS Management, expanding coverage to generative AI shadow IT discovery via the Shadow AI Dashboard, which gives visibility into generative AI app adoption, usage by department, and most-active users, with proactive approval or restriction controls that can act before apps are formally discovered. Originally launched for discovering, tracking, categorizing, and blocking shadow IT SaaS apps via the JumpCloud Go browser extension (no longer requiring JumpCloud Go enabled at the org level, only on end-user devices), with customizable warning or blocking messaging; also adds enforced approved SaaS access applying security, device trust, and access policies uniformly across every AI tool and app.

— Traces the feature's evolution and named dashboard but lacks an exact config path.

`Release Notes 2025 (2026-09-10)` `launch-20260910-918b8bcf`

`Release Notes 2024 (2026-09-10)`

---

10 **Custom Admin Role permission scopes renamed** BREAKING

72

Renames Custom Admin Role scopes: Policy Management becomes `Access Management`, System Management becomes `Devices`, and Authentication Policies becomes `Conditional Access Policies and IP Lists`. Admins must review existing custom

roles under `Roles > Custom Roles > [role] > Permissions` to confirm the renamed scopes still grant intended permissions.

Review and update a custom admin role after the scope renames to ensure the role still grants the intended permissions under the new names (Access Management, Devices, Conditional Access Policies and IP Lists).

> 📍 In the JumpCloud Admin Console, go to Roles › Custom Roles › select your role › Permissions, verify that previously configured scopes now appear as Access Management (was Policy Management), Devices (was System Management), and Conditional Access Policies and IP Lists (was Authentication Policies), and save any needed adjustments.

— Gives exact old/new scope names and the review path.

Roles Based Access Release Notes 2025 (…

---

11 **Step-up authentication and AMR claims for SSO** NEW

69

Honors `ForceAuthn='true'` in SAML and `prompt=login` in OIDC so applications can trigger step-up authentication without ending the user's existing session, and includes Authentication Methods References (AMR) claims in both SAML assertions and OIDC ID tokens, tagging logins with proof of factors used (e.g. password + OTP).

— Names exact protocol parameters and claim type; no config UI path given.

Release Notes 2025 (2026-09-10)

---

12 **User group exclusion from JumpCloud Protect Unified MFA** NEW

66

Adds User Group Exclusion from JumpCloud Protect Unified MFA, allowing specific groups to use TOTP only without Push enrollment, configured via `Security > MFA > JumpCloud Protect > User Group Exclusions` in the Admin Portal.

Exclude a regional user group from Push MFA enforcement so users in areas where Push is unavailable can authenticate with TOTP only.

> 📍 In the Admin Portal, go to Security › MFA › JumpCloud Protect, open User Group Exclusions, and add the target group to exclude it from Push enforcement.

— Names the exact settings path to exclude a group from Push MFA.

Release Notes 2025 (2026-09-10)

---

13 **Command After Agent Install command type** NEW

66

Adds a new Command After Agent Install command type; in Commands > New Command, admins select this type, paste an enrollment script, and it runs automatically on any newly enrolled device once the agent install completes.

Enroll a new device and immediately run a hardening script the moment the JumpCloud agent finishes installing, without waiting for a manual trigger.

> 📍 In the Admin Portal, go to Commands › New Command, select the `Command After Agent Install` command type, paste your enrollment script, and save. The command will execute automatically on any newly enrolled device once the agent install completes.

— Gives the exact command type and trigger behavior from the example.

Release Notes 2022 (2026-09-10)

---

14 **Asset Management gains invoice uploads, device accounts, and a scoped role**

NEW

65

Adds an `Invoice` field (File Upload type) under Purchase Details in Asset Management for uploading invoices or contracts to asset records, a `Local Device Accounts` section on the Asset Detail page under Device Management, and a new `Asset Manager` admin role scoped exclusively to Asset Management.

— Names all three added surfaces but no navigation path for each.

Release Notes 2025 (2026-09-10)

---

15 **JumpCloud Go passwordless login and default MFA policy** NEW

65

Adds the `JumpCloud Go` browser extension, enabling hardware-protected, phishing-resistant passwordless login to JumpCloud-protected web resources using Apple Touch ID and Windows Hello on managed macOS and Windows devices. Conditional access policies for SSO apps now default to JumpCloud Go as the MFA method, with user and device verification occurring on every application session.

— Names the auth mechanisms and default policy change; no setup steps given.

Release Notes 2023 (2026-09-10)

---

16 **Service Accounts for API integrations** NEW

64

Introduces Service Accounts for APIs — accounts not tied to individual admin accounts — improving the security and reliability of API integrations; create one via `Settings > Service Accounts` in the Admin Portal to generate an API key that replaces personal admin keys in automation scripts.

Scope an API integration to a non-personal service identity so that admin turnover no longer breaks your automation.

> 📍 In the JumpCloud Admin Portal, go to Settings › Service Accounts, create a new Service Account, generate an API key, and replace any personal admin API keys used in your integration scripts with the new key.

— Gives the exact Admin Portal path to create and use a service account key.

Release Notes 2025 (2026-09-10)

---

17 **Windows MDM policy framework using Configuration Service Providers**

NEW 64

Introduces a new Windows MDM policy framework using Configuration Service Providers (CSPs), with six new policies: Windows Wi-Fi Configuration, Windows VPN, Install Certificate, Bluetooth Configuration, Control Policy Conflict (enabled by default), and Windows Notification Service (enabled by default).

— Names all six new policies and their default states. Release Notes 2024 (2026-09-10)

---

18 **MCP servers must be assigned an SSO application in AI Gateway**

62

BREAKING

MCP servers in AI Gateway that were previously created without an associated SSO application or bookmark must now have one assigned — access is not scoped by User Groups until an application is assigned, and admins are prompted to assign one on next access. This affects servers added before August 21, 2026.

— Clear before/after and migration trigger, no exact remediation steps given.

Release Notes 2026 (2026-09-10) changelog-20260910-6fcef65f

---

19 **TOTP support for LDAP MFA** NEW 60

Adds TOTP as an MFA factor option for LDAP applications; admins enable MFA and select TOTP as an allowed factor under Directory > LDAP > [application] > MFA Settings, prompting users for a TOTP code on next login.

Require TOTP as a second factor for users authenticating into an LDAP application, without distributing push-notification capable devices.

> 📍 In the Admin Portal, go to Directory › LDAP › select your LDAP application › MFA Settings, enable MFA, and select TOTP as an allowed factor. Users will be prompted for their TOTP code on next login.

— Gives the exact Admin Portal path to enable TOTP for LDAP.

Release Notes 2022 (2026-09-10)

---

20 **Device Monitoring and Alerting across Windows, macOS, and Linux**

NEW 60

Introduces JumpCloud Device Monitoring and Alerting, enabling customizable alerts for device health (availability, software, uptime, disk, battery), policy/command/software

management results, directory events (user addition, privilege elevation), and command execution monitoring across Windows, macOS, and Linux.

— Names all monitored categories but no configuration path.

Release Notes 2024 (2026-09-10)

THINNER COVERAGE BELOW

21 **Multi-Tenant Portal admin and reporting capabilities** NEW

57

Adds Multi-Tenant Portal (MTP) Homepage widgets, including an aggregate reports widget bulk-exportable as JSON or CSV and an MDM Upcoming Certificate Expirations widget, and adds the ability for MSP admins to add new users and devices, export user and device lists, and perform bulk actions directly from the MTP.

— Names widgets and export formats but no exact navigation steps.

Release Notes 2023 (2026-09-10) Release Notes 2022 (2026-09-10)

22 **RADIUS certificate authentication and multi-IP configuration**

NEW

56

Supports certificate (passwordless) based authentication to JumpCloud RADIUS using any X.509-compliant certificate authority, allowing imported certificates to be used for RADIUS authentication, and adds support for multiple IP addresses in a single RADIUS server configuration.

— Names the certificate standard and config change but no setup steps.

Release Notes 2024 (2026-09-10) Release Notes 2022 (2026-09-10)

23 **Remote Assist unlimited access with unresponsive-agent handling**

IMPROVED

54

Adds JumpCloud Remote Assist for unlimited, free remote desktop access and support on Windows and macOS devices, requiring JumpCloud Agent v1.61.0 or later. Remote Assist now automatically detects and terminates unresponsive agent instances on end-user devices before establishing a new admin connection.

— Names the required agent version and unresponsive-agent behavior.

Release Notes 2024 (2026-09-10) Release Notes 2022 (2026-09-10)

24 **Directory Insights filters split for application and resource names**

IMPROVED

53

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

— Names every new sub-filter exactly, though usage context is thin.

Release Notes 2025 (2026-09-10)

25 **AI Commands Builder generates admin commands from prompts**

NEW 49

Launches AI Commands Builder, allowing admins to generate and refine commands for Windows, macOS, and Linux devices using natural-language prompts inside the Admin Portal.

— Names the OS targets and entry point but no exact UI path or example.

Release Notes 2025 (2026-09-10)

26 **Support case access in Admin Portal and Multi-Tenant Portal**

NEW 49

Adds the JumpCloud Case Portal to the Admin Portal Support menu, centralizing all organization cases and ideas in a filterable list, and extends Customer Portal access to MTP admins, letting them access, view, and create support cases for all tenant organizations managed by their MTP account.

— Names both entry points but no field-level or API detail.

Release Notes 2025 (2026-09-10) Release Notes 2022 (2026-09-10)

27 **New third-party integrations: SentinelOne and Deel SSO** NEW

48

Adds the SentinelOne integration, allowing the SentinelOne Agent to be downloaded and installed on macOS, Windows, and Linux devices via JumpCloud Commands, and adds a Deel SSO Connector integration enabling admins to create a Deel SSO integration.

— Names both integrations and the deployment mechanism for one.

Release Notes 2023 (2026-09-10) Release Notes 2022 (2026-09-10)

28 **Frequency-based alert triggers in Insights Rules** IMPROVED

44

Alert trigger conditions in Insights Rules can now fire based on event frequency thresholds rather than every individual event, letting admins define specific criteria for when an alert fires and reducing alert noise.

— Describes the mechanism but gives no exact UI path or threshold values.

Release Notes 2026 (2026-09-10) changelog-20260910-6fcef65f

29 **Quick navigation keyboard shortcut in Admin Portal** NEW

44

Adds a keyboard shortcut (`⌘/Ctrl + K`) in the Admin Portal for quick navigation and search.

— Gives the exact shortcut, though scope of what it searches is unstated.

Release Notes 2024 (2026-09-10)

30 **Self Service App Catalog reaches GA** IMPROVED 42

Self Service App Catalog is now generally available for macOS and Windows, letting users install JumpCloud App Catalog applications directly from their devices via Software Management.

— States GA scope and access path but no further mechanism. changelog-20260910-6fcef65f

31 **Custom Admin Roles for all direct organizations** NEW 36

Introduces Custom Admin Roles for all direct organizations, enabling granular role creation and assignment based on specific responsibilities.

— States the capability but no scopes or navigation named.

Release Notes 2025 (2026-09-10)

32 **Faster EAP reconnect via cached session credentials** IMPROVED 36

Adds faster reconnect for EAP connections by caching session credentials to skip the full security handshake on reconnect, allowing recently authenticated devices to reconnect faster.

— Explains the mechanism but gives no configuration or measurable improvement.

Release Notes 2025 (2026-09-10)

33 **Identity First Login for User Portal and SSO apps** NEW 36

Introduces Identity First Login for the User Portal and SSO applications, splitting authentication into a username/email screen and a separate password screen.

— States the flow change but no configuration or rollout detail.

Release Notes 2022 (2026-09-10)

34 **Account-Driven User Enrollment for BYOD iOS/iPadOS reaches GA**

IMPROVED 36

Adds support for Account-Driven User Enrollment (ADUE) for BYOD iOS/iPadOS 18+ devices in MDM, now generally available.

— States GA scope and OS version but no enrollment steps. Release Notes 2024 (2026-09-10)

35 **M365/Azure AD security group support in Microsoft 365 integration**

NEW 28

Adds M365/Azure AD security group support to the JumpCloud Microsoft 365 directory integration.

— A bare one-line addition with no further mechanism given.

Release Notes 2022 (2026-09-10)

└──▷ ALSO FROM THESE RELEASES

Block unwanted macOS 13 Ventura upgrades across your fleet while still allowing security patch updates.

📍 In the Admin Portal, go to Device Management › Policies › New Policy › macOS › select the Ventura delay/block software management policy, configure your deferral window, and bind the policy to the target device group.

Subscribe to only agent and product release note updates so your RSS reader filters out general Help Center noise.

📍 1. Go to the JumpCloud Release Notes and Bug Fixes page. 2. Click `Subscribe to Release Notes and Bug Fixes RSS Feed`. 3. Open your RSS reader and add the resulting feed URL to receive product release notes and agent release note updates automatically.

└──▷ BREAKING ON UPGRADE

- ! The `GET /systemusers/reactivate/{id}` endpoint is deprecated and now returns a 404 error; all scripts, automations, and integrations must switch to `POST /systemusers/reactivate/{id}` with `activation_email` in the request body.
- ! The `$le` and `$ge` filter operators for Dynamic Groups `memberQuery` API filters are deprecated in favor of `$lte` and `$gte`; API integrations using these operators must be updated.
- ! MCP servers in AI Gateway that were previously created without an associated SSO application or bookmark must now have one assigned — access is not scoped by User Groups until an application is assigned, and admins are prompted to assign one on next access.
- ! The Policy Management scope is renamed to Access Management; any roles or documentation referencing Policy Management must be updated.
- ! The System Management scope is renamed to Devices; any roles or documentation referencing System Management must be updated.
- ! The Authentication Policies scope is renamed to Conditional Access Policies and IP Lists; any roles or documentation referencing Authentication Policies must be updated.

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

! MCP servers added before August 21, 2026 that have no associated SSO application or bookmark must be assigned one in AI Gateway — access is not scoped by User Groups until an application is assigned.

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

WAS THIS USEFUL? 👍 👎

ConductorOne

Feedback ⓘ 2 RELEASES · 2026-09-10 CHANGELOG ↗

RANK

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

> ConductorOne's biggest addition this window is a dedicated Non-Human Identity dashboard, alongside a full admin navigation reorganization with per-section overview pages, new MCP server resource governance and guided setup, role mining and findings-reprocessing improvements, and two breaking changes to automation expressions and finding field naming.

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

01 **Non-Human Identity (NHI) overview dashboard** NEW 88

Adds an `Identities > Overview` dashboard surfacing every human and non-human identity discovered across connected sources, with a dedicated `NHI` tab scoped to app registrations (Entra enterprise apps, OAuth apps, GitHub Apps, Databricks service principals), assumable roles (AWS IAM roles, GCP workload identities), and managed identities, plus separate `Human users`, `Service`, `Secrets`, and `Agents` tabs. Shows type/subtype strings (e.g. `entra.enterprise_application`, `aws.role.lambda`), owner, and open findings per identity, highlights unowned NHIs as findings with evidence, remediation guidance, and activity trail, and supports filtering by app, owner, type, or `Has findings`, plus name search.

Quickly find all unowned non-human identities across your connected apps to close a common access governance gap.

> 📍 In the ConductorOne console, go to Identities › Overview, select the NHI tab, then apply the filter Has findings to surface every app registration, assumable role, or managed identity without an assigned owner.

— Full mechanism, named identity categories and filters, exact UI path product docs

02 **Admin navigation reorganization with per-section dashboards**

IMPROVED 78

Adds a new `Platform` section housing `Policies`, `Forms`, `Task log`, and `Integrations` (excluding `Connectors`); adds a per-section Overview dashboard for every nav section except `Apps`, replacing the single Analytics/Product digest view; moves `Connectors` into `Apps` and `Automations` into `Governance`; renames `Directory` to `Identities` and `Identity security` to `Security`, which now also houses `Decoys` and the `Graph` explorer.

Find per-app governance and connector config in one place after the nav reorganization.

> 📍 In the C1 admin console, go to Apps › Connectors to manage connector configuration alongside app governance.

Access the new per-section Overview dashboard to replace the single Analytics page.

> 📍 In the C1 admin console, select any section (e.g., Security, Governance, Identities) and click its Overview page to view the section-scoped dashboard.

— Names every moved/renamed nav section with UI paths `Updated navigation (2026-09-10)` `changelog-20260910-87306871`

---

03 **Bulk entitlement request limit in Forms** NEW 78

Adds a bulk request limit setting in `Governance > Forms` letting admins cap the number of entitlements a user can request at once, configurable from 1–100 with a default of 10.

Cap the number of entitlements users can bulk-request at once to reduce over-provisioning blast radius.

> 📍 In the C1 admin console, go to Governance › Forms › Configure tenant-wide request settings and set the bulk request limit to a value between 1 and 100 (default is 10).

— Exact config path and value range given, runnable steps `changelog-20260910-87306871`

---

04 **MCP static resource and URI template governance** NEW 63

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

— Mechanism described, no UI path or example `changelog-20260910-87306871`

---

05 **SSO silent, fresh, and passive authentication handling** IMPROVED 60

Supports OIDC silent and fresh authentication requests and SAML passive requests in SSO applications, returning an error instead of silently reusing a session when a request cannot be completed safely.

— Behavior change is clear, no config surface named `changelog-20260910-87306871`

THINNER COVERAGE BELOW

06 **Role mining threshold and routing improvements** IMPROVED

52

Adds a configurable shared-access threshold, pre-action entitlement list refinement, and optional access request task routing for automatic profile enrollments to role mining.

— Names three improvements, no exact config values changelog-20260910-87306871

---

07 **Manual deprovisioning fallback for unsupported revokes**

IMPROVED

47

Revokes on connectors that cannot deprovision a given entitlement now route to manual deprovisioning instead of closing as Revoked with no source change.

— Before/after behavior stated, no config surface changelog-20260910-87306871

└──▷ **ALSO FROM THESE RELEASES**

└──▷ **BREAKING ON UPGRADE**

! Automation expressions consisting of the bare workflow context, or that pass it to a function, no longer compile — expressions must reference the step and field directly. Existing running automations are unaffected until next edited and saved, at which point indirect-reference expressions must be rewritten to a static path.

! The Owner column, filter, detail field, and corresponding API/webhook field and audit-log event names on findings are renamed to Assignee. Consumers of the Finding object via API, webhook, or SIEM audit log must update to the new field and event names.

WAS THIS USEFUL? 👍 👎

SailPoint

Feedback

1 RELEASE · 2026-09-09

BLOG ↗

RANK

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

> SailPoint expanded its connector catalog with ten new integrations and rolled out platform-wide Dark Mode support with custom branding.

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

01 **Dark Mode across Identity Security Cloud** NEW 55

Enables Dark Mode across Identity Security Cloud, including SailPoint Agentic Fabric and most ISC modules. Supports custom brand colors in Dark Mode with automatic switching between Light and Dark modes based on existing brand configuration, and adds color pickers for branding configuration. Dark Mode configured in ISC extends automatically to Data Access Security (DAS) with no additional configuration required.

— Explains scope and behavior but no config path Enhancement: Dark Mode Updates (2026-09…

02 **Ten new native connectors** NEW 50

Adds native connectors for `Absence.io`, Attio, `FreeAgent`, `GitGuardian`, Holded, Movidesk, Ploomes, `ProdPad`, `SOTI MobiControl`, and `StatusGator`, extending identity governance coverage to these platforms.

— Names all ten connectors but no setup detail product docs

WAS THIS USEFUL? 👍 👎

BeyondTrust

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

BeyondTrust provides privileged access management and endpoint security solutions for controlling and monitoring user access to critical systems.

> Integration Client 26.2.1 adds tunable HTTP timeout config keys and new session asset columns for reporting, while removing username/password API authentication from Site Configuration in favor of Client ID/Secret.

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

01 **Configurable HTTP request timeouts** NEW 86

New config keys `DownloadTimeoutSeconds`, `ApiRequestTimeoutSeconds` (default: 300 s), and `ApiInfoTimeoutSeconds` (default: 60 s) bound and tune HTTP timeouts per environment, preventing the client from hanging against a slow appliance.

Prevent the client from hanging indefinitely against a slow appliance by setting explicit timeouts for each request class.

ini

```
DownloadTimeoutSeconds = 600
ApiRequestTimeoutSeconds = 120
ApiInfoTimeoutSeconds = 30
```

— Named config keys with defaults and a runnable example

Integration Client 26.2.1 release notes…

02 **Session asset columns in reporting plugins** NEW 72

Adds four nullable session columns — `asset_type`, `asset_name`, `asset_comments`, and `asset_tag` — to both the Analytics DB Plugin and the SQL Server Plugin, populated from the Reporting API, letting reporting teams correlate session activity with the worked-on asset without joining an external inventory source.

— Names exact columns and plugins but no direct action step

Integration Client 26.2.1 release notes…

03 **API authentication now requires Client ID and Secret** BREAKING 65

The User Account / API Account toggle is removed from Site Configuration — every site must now be configured with a Client ID and Client Secret; any site that relies on username and password API authentication must be reconfigured before it will function.

— Clear migration note but no exact UI path or endpoint

Integration Client 26.2.1 release notes…

└──▷ BREAKING ON UPGRADE

! The User Account / API Account toggle is removed from Site Configuration — every site must now be configured with a `Client ID` and `Client Secret`; any site that relies on username and password API authentication must be reconfigured before it will function.

WAS THIS USEFUL?  

1Password

Feedback ⓘ 6 RELEASES · 2026-09-09 BLOG ↗ RANK

All the latest releases from the 1Password team

> 1Password's September 9 releases focused on developer tooling and platform-specific security defaults: Developer Environments gained CLI/SDK access and environment ID copying across Linux, Mac and Windows betas, Linux added a per-request SSH approval setting, macOS expanded and made Autofill more controllable, Windows now defaults to TPM-backed Windows Hello, iOS streamlined biometric unlocking across accounts, and the browser extension picked up split-screen login saving and diagnostic/UI polish.

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

01 Expanded macOS Autofill with disable toggle IMPROVED

75

macOS Autofill now works in more places, including when connecting to a server in Finder, showing a confirmation prompt before filling; a new `Settings > Autofill > 'Disable macOS Autofill'` option lets users turn macOS Autofill off entirely from within the app.

Disable macOS Autofill if it is triggering in unwanted contexts after the expanded coverage in this release.

📍 In 1Password, go to Settings › Autofill › Disable macOS Autofill.

— Names exact settings toggle path with a usage example.

1Password for Mac beta 8.12.38-25 (2026…

02 CLI/SDK programmatic access in Developer Environments NEW

60

Developer Environments now includes programmatic access options for the 1Password CLI and SDKs, plus an option to copy the environment ID, so developers can pull environment credentials into scripts or SDK-based workflows. Shipped across the Linux, Mac and Windows betas.

Access CLI and SDK credentials directly from Developer Environments to integrate 1Password secrets into automated workflows.

📍 In 1Password, go to Developer Environments, open an environment, then use the programmatic access options to configure the 1Password CLI or SDKs, and copy the environment ID for use in scripts.

Retrieve the environment ID for a Developer Environment to use with the 1Password CLI or an SDK in automated pipelines.

> 📍 In 1Password for Windows, go to Developer › Environments, open the target environment, then use the `Copy environment ID` option and the programmatic access panel to get the CLI or SDK credentials.

– Named feature across three platforms, but no exact CLI command shown.

`1Password for Linux beta 8.12.38-25 (20…` `1Password for Mac beta 8.12.38-25 (2026…` `1Password for Windows beta 8.12.38-25 (…`

THINNER COVERAGE BELOW

03 TPM support on by default with Windows Hello IMPROVED

50

When `Unlock using Windows Hello` is turned on, the Convenient and Balanced security presets now turn on Trusted Platform Module (TPM) support by default.

– Describes the default change but requires no user action.

`1Password for Windows beta 8.12.38-25 (…`

04 Single Face ID unlock for all accounts in Autofill IMPROVED

45

Improves Autofill unlocking on iOS so one Face ID prompt unlocks every available account, and skips biometric prompts when an account requires a password instead.

– Clear behavioural change described but no navigation steps given.

`1Password for iOS beta 8.12.38-25 (2026…`

05 Simplified account setup with clearer SSO errors IMPROVED

35

Simplifies the steps to add an account from 1Password.com or via QR code scanned with 1Password on a mobile device, and SSO account-add errors now show a specific error message instead of a generic one.

– Combines two thin account-setup tweaks without further specifics.

`1Password for Linux beta 8.12.38-25 (20…`

06 Save logins on split username/password screens NEW

35

1Password in the browser now offers to save your login when a site asks for your username and password on separate screens.

– Describes the scenario handled but no config or steps given.

`1Password in the browser 8.12.38-25 (20…`

07 **Breadcrumb navigation in Developer Watchtower** IMPROVED

25

The Developer Watchtower page now includes breadcrumb navigation.

— Thin one-line addition with no further detail on scope.

1Password for Linux beta 8.12.38-25 (20…

08 **Browser extension version indicator** NEW

25

Settings now shows whether the browser extension is connected to 1Password 7 or 1Password 8.

— Bare mention of a diagnostic indicator, no further detail.

1Password in the browser 8.12.38-25 (20…

09 **Redesigned SSO migration prompt** IMPROVED

15

Visual improvements to the single sign-on (SSO) migration prompt with a simpler, more compact design.

— Vague description of a visual redesign with no specifics.

1Password in the browser 8.12.38-25 (20…

WAS THIS USEFUL? 👍 👎

Didit

Feedback

ⓘ

1 RELEASE · 2026-09-10

CHANGELOG ↗

RANK

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

> Didit expanded non-document identity verification with per-country method controls, failure-mode routing, automatic liveness for portrait-return lookups, and configurable retry limits, while surfacing verification method and assurance tier in its decision API and webhooks.

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

01 Per-country method controls and failure-mode routing NEW

88

A new Countries tab on the ID Verification step lets teams toggle document capture, non-document lookup, and digital wallet methods on or off per country, with the same controls available via the API. For each non-document method, per-failure-mode switches (partial match, no match, no source response, wallet cancelled/timed out) route the user to document capture or decline the session.

Enable non-document lookup for specific countries via the console so users in those countries can verify without uploading a document.

📍 In the console, open your workflow, select the ID Verification step, go to the Countries tab, find the target country row, and toggle Non-document lookup on. Set the per-failure-mode switches (partial match, no match, no response) to either Fall back to document capture or Decline session, then save.

— Exact UI path and failure-mode options given changelog-20260910-7d1f33ab

02 SDK_VERSION export in Web SDK IMPROVED

83

`@didit-protocol/sdk-web` now exports `SDK_VERSION` that correctly reflects the installed package version across all build formats and TypeScript declarations; upgrade with `npm install @didit-protocol/sdk-web@latest` to also pick up an embedded-mode sizing fix.

Upgrade the Web SDK to 0.3.1 to get the corrected `SDK_VERSION` and the embedded-mode sizing fix.

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

— Exact package name and install command given changelog-20260910-7d1f33ab

03 **Automatic liveness and face-match for portrait-return lookup countries**

IMPROVED 78

For lookup countries whose government register returns a portrait (South Africa, Nigeria, Argentina, Panama), the non-document lookup automatically adds passive liveness and face-match, included in the lookup price, letting teams skip the separate downstream Liveness and Face Match workflow steps.

— Named countries and price inclusion, no config step shown changelog-20260910-7d1f33ab

---

04 **Verification method and assurance tier in decision API and webhooks**

NEW 70

The `status.updated` webhook payload and decision API now include fields carrying the verification method (Documentary , Data match , Cryptographic) and the assurance tier for every ID Verification session.

— Named fields but no endpoint path or example given changelog-20260910-7d1f33ab

---

05 **Registry comparison and credential detail result views** NEW 65

Verification results now include a Registry comparison detail showing every field comparison — what the user provided, what the source held, and whether it matched — plus an error row when a source did not respond. Wallet verifications get a Credential details view showing wallet identity, issuing authority, level of assurance asserted, and signature validity.

— Named result fields but no navigation path given changelog-20260910-7d1f33ab

---

06 **Configurable lookup retry count** NEW 65

Non-document lookup retry count is now configurable from one to five attempts (default two); only attempts the source actually answered are counted and billed.

— Numeric limits given but no exact config key named changelog-20260910-7d1f33ab

THINNER COVERAGE BELOW

---

07 **Digital ID wallet verification method** NEW 50

Adds digital ID wallet as a configurable ID Verification method (MitID, BankID, itsme, Vipps, iDIN, UAE PASS, gov.br, EUDI Wallet), surfaced as Coming soon in the console and not yet enabled for production users.

— Feature listed as coming soon, not yet usable changelog-20260910-7d1f33ab

WAS THIS USEFUL?

Ory

Feedback

1 RELEASE · 2026-09-10 NOTES ↗ RANK

Ory delivers identity and access management (IAM) for applications, enterprises, and AI agents. Cloud-native, API-first, and self-hostable.

> Ory shipped a temporary workaround for firewalls that reject post-quantum TLS handshakes triggered by its services offering ML-DSA post-quantum signatures.

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

01 Workaround for post-quantum TLS firewall rejections IMPROVED

35

Ory Network v26.3.13 adds a temporary workaround for firewalls that reject post-quantum TLS handshakes caused by Ory services offering ML-DSA post-quantum signatures.

— Names the mechanism (ML-DSA) but no config or migration steps given.

Ory Network,Ory Hydra, Ory Kratos, Ory …

WAS THIS USEFUL?

Auth0

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

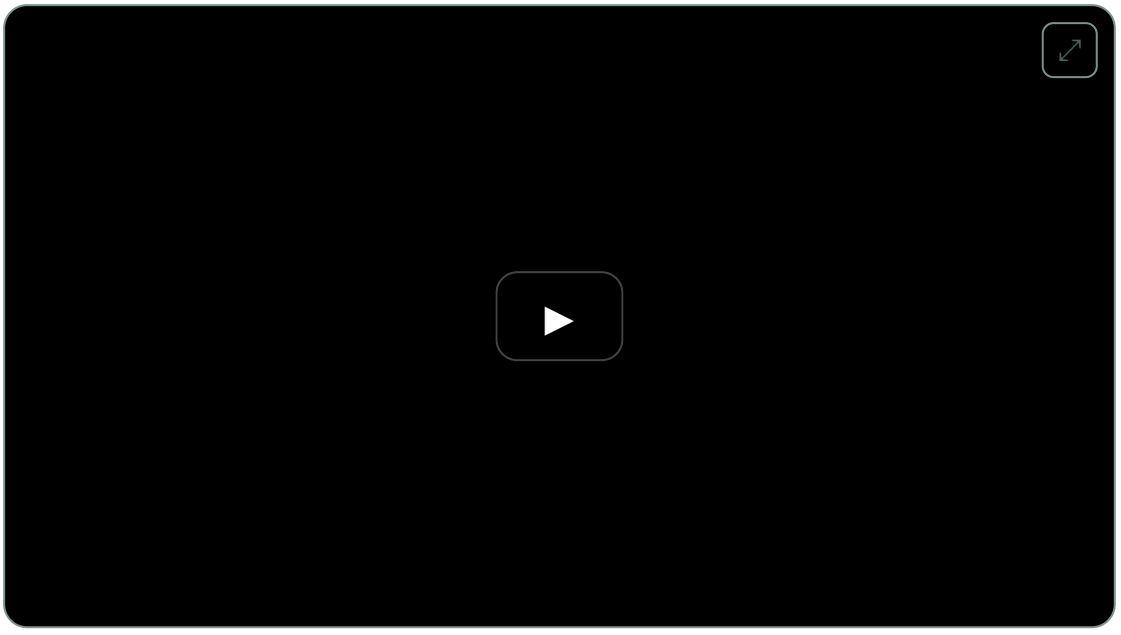
Secure users, AI agents, and more with Auth0, an easy-to-implement, scalable, and adaptable authentication and authorization platform.

> Auth0 introduced Agent Skills, a package of AI coding-agent skills including an automated tenant security and configuration audit (HealthCheck) and dozens of framework-specific quickstart modules.

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

01 **HealthCheck skill for tenant security audits** NEW 88

The `Auth0 HealthCheck` skill, installed via `npx skills add auth0/agent-skills`, queries a live Auth0 tenant through the Auth0 Management API and Auth0 CheckMate to produce confidence-weighted security posture and capability-fit scores, generating a prioritized findings report. Automated scans cover token signing algorithms (RS256 vs HS256), DPoP configuration, CORS origins, attack protection settings, callback URLs, logout redirects, social connection keys, grant types, and database connection settings.



Install Auth0 Agent Skills into your local AI coding environment so your agent can audit live tenant configuration instead of guessing.

```
$ npx skills add auth0/agent-skills
```

— Names install command, API, and every scanned config area launch-20260908-1858357a

THINNER COVERAGE BELOW

02 **Framework quickstart skill modules** NEW 46

Auth0 Agent Skills ships 35+ framework quickstart skill modules that detect the application framework in use and load relevant SDK guidance, with support named for React, Next.js, Node.js, Python, Swift, Flutter, and more.

— Lists frameworks but no usage detail beyond install `launch-20260908-1858357a`

WAS THIS USEFUL? 👍 👎

◆ Data Security & DLP

Immuta

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

Use Immuta to provision governed access to data.

> Immuta's Request app gained bulk multi-user access requests and an email-hover tooltip to disambiguate similarly named users.

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

01 **Bulk multi-user access requests** NEW 60

The Immuta Request app now supports requesting access for multiple users in a single submission, replacing the need to create separate requests per person. A requester can select all relevant users from the user picker, fill in the request details once, and submit a single request covering the entire group.

When a manager needs to onboard a team to a data product at once, submit a single group access request instead of repeating the process for each person.

> 📍 In the Immuta Request app, open the request form, select all relevant users from the user picker, fill in the request details, then click Submit once to cover the entire group.

— Describes workflow and before/after but no API or config detail `snapshot-20260910`

THINNER COVERAGE BELOW

02 **Email tooltip for user names in requests** NEW 35

Hovering over a user name in the Immuta Request app now displays that user's email address, helping disambiguate users with similar or identical names.

— Simple UI addition with no configurable surface named `snapshot-20260910`

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

DNSFilter

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

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

> DNSFilter's MCP Server integration is now generally available, letting AI assistants query DNS data and manage policies through natural language.

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

01 **DNSFilter MCP Server general availability** NEW 80

The DNSFilter MCP Server integration is reachable under Integrations → AI Connectors and lets AI assistants (Claude, ChatGPT, Codex) query DNS activity and threat data, manage policies and allow/block lists, and automate reports and investigations via the Model Context Protocol, without dashboard navigation. Connected MCP clients stay authorized for seven days before requiring reconnection, and operate under the connecting user's existing DNSFilter permissions.

Connect an AI assistant to DNSFilter so you can query threat data and manage block lists in natural language without opening the dashboard.

> 📍 In DNSFilter, go to Integrations → AI Connectors, open the DNSFilter MCP Server card, copy the server URL, then follow the MCP Server setup guide to register that URL as the MCP server in your AI client (Claude, ChatGPT, or Codex). Setup requires an admin account.

— Names UI path, auth duration and permission model, but no API details.

09/09 September 9 – DNSFilter MCP Serve…

WAS THIS USEFUL? 👍 👎

Zscaler

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

Zscaler is a cloud-based security platform that inspects and filters internet traffic to protect against threats and enforce security policies.

> Zscaler extended its Zero Trust Browser Extension to enforce existing web policies inside the ChatGPT desktop app's embedded Chromium browser on macOS and Windows.

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

01 Zero Trust Browser Extension in ChatGPT embedded browser NEW

88

The Zero Trust Browser Extension now runs inside the ChatGPT desktop app's embedded Chromium browser on macOS and Windows, enforcing the same policies already used in Chrome, Edge, Firefox and Safari — DLP, paste controls, URL category blocking, file upload/download, credential protection, and tenant restrictions — with no separate rulebook for the embedded case. Deployment uses the same MDM-based method as other browsers but requires an explicit change to the deployment script to target the ChatGPT desktop app's embedded browser, since installing for Chrome does not cover it automatically. Agent-driven page loads appear in the Zscaler admin console as standard detections carrying user identity, device posture, extension version, browser, IP, geolocation, and URL, and the Paste Blocked and Content Blocked interstitials render in-page when policies trigger.

Start with full visibility before writing block rules — log every page the ChatGPT agent opens without blocking anything.

> 📍 In the Zscaler Zero Trust Browser admin console, create a policy named Monitor All Website Visits with a single catch-all rule: Condition: page.url exists | Effect: Allow | Severity: Informational. Assign it to the target user group covering ChatGPT desktop app users.

Prevent users from pasting sensitive data into a known DLP test site when ChatGPT opens it in the embedded browser.

> 📍 In the Zscaler Zero Trust Browser admin console, create a policy named Block Paste on DLP Test Site with rule: Condition: `page.url.domain` is equal to dlptest.com | Effect: Block | Severity: Medium. Assign to the relevant user group.

Block entire URL categories (e.g., Gambling) for ChatGPT agent browsing so that category-aware blocks catch retry attempts across domains.

> 📍 In the Zscaler Zero Trust Browser admin console, create a policy named `Block Gambling websites` with rule: Condition: `page.url.category` is one of Gambling | Effect: Block | Severity: Medium. Assign to the relevant user group.

— Names mechanism, deployment change, admin console fields, and runnable policy examples.

2026-09-09-787f5194

WAS THIS USEFUL? 👍 👎

tailscale

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

The easiest, most secure way to use WireGuard and 2FA.

> Tailscale's Kubernetes Operator 1.102 adds a new PeerRelay CRD for automated in-cluster peer relays, extends ProxyGroup Egress to IPv6 destinations, and tightens up Let's Encrypt certificate issuance.

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

01 PeerRelay CRD for in-cluster peer relays NEW

93

The Kubernetes Operator can now deploy and manage in-cluster Tailscale peer relays via a new `PeerRelay` custom resource (`apiVersion: tailscale.com/v1alpha1`, `kind: PeerRelay`), with support for `spec.replicas`, tags, `proxyClass` inheritance, and `tailnet` configuration.

Deploy a highly-available in-cluster peer relay in a VPC-isolated cluster to facilitate direct cross-cluster connections without manual Tailscale client configuration.

yaml

```yaml
apiVersion: tailscale.com/v1alpha1
kind: PeerRelay
metadata:
  name: my-relay
spec:
  replicas: 2
```

— Full CRD schema plus a runnable example manifest. launch-20260909-f3f249ae

THINNER COVERAGE BELOW

02 IPv6 destinations for ProxyGroup Egress IMPROVED

55

`ProxyGroup` Egress now supports IPv6 destinations, including 4via6 subnet routers — previously only IPv4 destinations were valid.

— Names the surface and before/after but no example. launch-20260909-f3f249ae

03 Let's Encrypt cert issuance optimizations IMPROVED

55

Certificate issuance for multiple domains now runs in parallel instead of serially, preventing provisioning of many domains from stalling behind each other. During Ingress deletion, VIPServices are now blocked from acquiring new certificates, avoiding wasted Let's Encrypt rate-limit quota in ephemeral deployments.

— Describes behavior change with no config surface to act on. launch-20260909-f3f249ae

WAS THIS USEFUL?  

GOVERNANCE, RISK & COMPLIANCE

◆ Continuous Control Monitoring (CCM)

RegScale

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

RegScale is a compliance management platform that automates regulatory reporting, audit preparation, and governance workflows for organizations.

> RegScale added Artifact Hub for templated, recurring compliance artifact generation and gave the CLI configurable console log formatting, alongside a small breaking change to `jcam` help output.

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

01 **Configurable CLI console log format** NEW 85

Adds `logFormat` and `logDateFormat` keys to `init.yaml` to configure console log output format and date format, overridable via `REGSCALE_LOG_FORMAT` and `REGSCALE_LOG_DATEFORMAT` environment variables, with environment values taking precedence over the config file.

— Names exact config keys and env vars with precedence rule. CLI 6.45.0 (2026-09-09)

THINNER COVERAGE BELOW

02 **Artifact Hub for templated artifact generation** NEW 58

A new workflow for creating reusable artifact templates, marking fields that change over time, and generating updated artifacts through a guided process. Ships with 16 ready-to-use templates for standardized artifact creation out of the box.

When you need to generate a recurring compliance artifact (such as a monthly evidence package) from a standardized template without rebuilding it each time.

> 📍 In RegScale, go to Artifact Hub, select one of the 16 ready-to-use templates, mark the fields that change each cycle, then follow the guided workflow to generate an updated artifact.

— Names workflow and template count but no deeper mechanism.

RegScale 6.34.0.1 (2026-09-09)

03 **jcam help listing drops renamed spellings** BREAKING 50

`jcam --help` no longer lists the pre-rename spellings `check_custom_fields` and `test_jcam`, reflecting an underlying command rename.

— States exact old names removed but not their new spellings. CLI 6.45.0 (2026-09-09)

└──▷ **BREAKING ON UPGRADE**

! `jcam --help` no longer lists the pre-rename spellings `check_custom_fields` and `test_jcam`.

WAS THIS USEFUL?  

◆ Third-Party & Vendor Risk (TPRM)

Conveyor

Feedback ⓘ 5 RELEASES · 2026-09-02 → 2026-09-04 NOTES ↗

RANK

Conveyor delivers AI for high-stakes customer requests like security reviews, vendor assessments, and requests for proposal (RFP).

> Conveyor's biggest window feature is the new agentic answering engine, now available for RFP proposals and in Labs for security questionnaires, alongside a rebuilt Word workflow, Slack-native questionnaire approvals, and self-serve automation rule editing.

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

01 Agentic answering engine for RFPs and questionnaires NEW

80

A new agentic answering engine can be enabled for RFP projects via `Settings > Answering > Custom Instructions`, replacing the prior answering pipeline with an agentic one selectable from a pipeline dropdown. Security questionnaire teams can now trial the same engine, currently in Labs, by creating a Test project.

Activate the new agentic answering engine so your team gets higher-quality, AI-driven answers on RFP proposal questions.

> 📍 In the Conveyor console, go to Settings › Answering › Custom Instructions and enable the new agentic engine.

Switch your RFP projects to the deeper agentic pipeline to reduce weak answers on high-stakes proposals.

> 📍 1. Log in as an Admin. 2. Go to Settings › Answering › Custom Instructions. 3. Open the pipeline dropdown and select Agentic. 4. Save. All new proposal questions will now use the agentic pipeline.

— Exact settings path and steps given, but no metrics on answer quality

🤖 New Agentic Answer Engine, Now Opt-I… 🏆 ConveyorAI for RFPs: The Whole Produ…

02 Self-serve automation rule editing NEW

80

Admins can now edit automation rule settings — Content In Scope, Number of Questions, Update Requests, Answer Status Check, and Return complete materials to source — directly on the Automation Rules page under `Settings > Workflow Automation > Automation Rules`, without filing a support request.

Tune your Slack intake workflow — adjust which content is in scope, how many questions are handled, and what gets returned on completion — without waiting on support.

> 📍 Go to Settings › Workflow Automation › Automation Rules, then edit Content In Scope, Number of Questions, Update Requests, Answer Status Check, or Return complete materials to source in place.

— Names every editable setting and exact navigation path

⚙️ Edit Your Own Automation Rules, No T…

03 **Slack-native questionnaire answer approval** NEW 75

Assigned reviewers now receive a rich Slack notification with the draft answer and buttons to approve or edit in-channel, with results synced back to Conveyor; existing customers enable this per program under `Settings > Self-Serve via Slack`.

Existing customers turning on Slack approvals for a specific questionnaire program.

> 📍 1. In Conveyor, go to Settings. 2. Select the questionnaire program you want to enable. 3. Open Self-Serve via Slack and toggle the feature on. 4. Reviewers assigned to questions will now receive draft answers in Slack with Approve or Edit buttons.

— Full workflow and exact settings path, missing rollout scope

💬 Approve Questionnaire Answers Straig…

THINNER COVERAGE BELOW

04 **Separate preview and download analytics in Trust Center** IMPROVED 45

Document previews and downloads are now tracked as separate actions in Trust Center analytics and reporting, replacing the previous behavior where previewing a PDF counted as a download.

— Clear before/after behavior but no reporting UI path given

🔧 Small Upgrades: Legacy Role Guidance…

05 **Rebuilt Word document experience for proposals** IMPROVED 40

RFP proposals now use a rebuilt Word document experience with improved loading, parsing, and export.

— Describes what changed but no steps or specifics on parsing changes

🏆 ConveyorAI for RFPs: The Whole Produ…

06 **Legacy role migration guidance** IMPROVED 35

The Roles page now shows a banner and inline help links prompting admins to migrate users off legacy roles to customized roles.

— Names the Roles page but no migration mechanics detailed

🔧 Small Upgrades: Legacy Role Guidance…

07 **Unified proposal workspace** NEW 30

A unified proposal workspace now runs RFPs and security questionnaires from a single Conveyor knowledge base.

— States the capability but gives no navigation or usage detail

🏆 ConveyorAI for RFPs: The Whole Produ…

08 **NDA signature alerts in Slack** NEW 25

Conveyor now sends a Slack message when a visitor signs your NDA, surfacing the buying signal without requiring a manual app check.

— States the trigger but no setup or configuration steps

🔧 Small Upgrades: Legacy Role Guidance…

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

ai-safe2-framework

Feedback ⓘ 1 RELEASE · 2026-09-10

NOTES ↗ RANK

Ai-Safe2-Framework provides governance, risk, and compliance controls for securing agentic AI systems and non-human identities.

> safe2 CLI 0.2.0 introduces offline Challenge evidence bundle generation and verification with fingerprint pinning, broadens Skill Trust Gate scanning to unrecognized file types, and adds an executable-isolation flag for the SkillSpector adapter, alongside breaking changes to the skill-gate script and AISM ingestion validation.

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

01 **Evidence bundle verification with fingerprint pinning** NEW

93

Adds `safe2 challenge verify-bundle <dir>` to verify an evidence bundle's internal consistency, rejecting missing or changed artifacts, unsupported versions, and inconsistent results. The `--expected-sha256` flag pins a complete bundle against a trusted manifest fingerprint obtained out-of-band.

— Named command and flag with exact failure conditions listed. 2026-09-09_safe2_CLI_0.2.0

02 **Offline Challenge evidence bundle generation** NEW 85

Adds `safe2 challenge quickstart 001 --output-dir <dir>` to generate an offline Challenge 001 evidence bundle with a Decision Card, requiring no model credentials or paid APIs.

— Runnable command with flags and stated no-credential behavior.

2026-09-09_safe2_CLI_0.2.0

03 **Skill-gate script replaced by CLI subcommand** BREAKING

75

The retired standalone skill-gate script now exits with an error; replace it with `safe2 gate skill PATH --strict`.

— Exact replacement command gives a clear migration path. 2026-09-09_safe2_CLI_0.2.0

04 **Expanded Skill Trust Gate scanning coverage** IMPROVED

65

The Skill Trust Gate now inspects scripts, extensionless files, and text with unfamiliar extensions — not just files with recognized extensions — covering injection directives, credential paths, and dynamic execution patterns.

— Describes scan scope expansion but no flag or command given. 2026-09-09_safe2_CLI_0.2.0

05 **Stricter AISM ingestion validation** BREAKING 65

AISM ingestion now rejects ambiguous JSON, unsafe paths, invalid Challenge runs, and existing output files — use a new output filename on each run.

— Lists rejection conditions and workaround, no named flags. 2026-09-09_safe2_CLI_0.2.0

06 **Executable isolation flag for SkillSpector adapter** NEW 60

Adds `--executable` flag to the SkillSpector adapter for running the provider in a separate environment.

— Names flag but isolation mechanism left unexplained. 2026-09-09_safe2_CLI_0.2.0

THINNER COVERAGE BELOW

07 **Release CI coverage for Python 3.11–3.14** IMPROVED 30

Extends release CI coverage to Python 3.11 through 3.14.

— Bare version-range statement with no further detail. 2026-09-09_safe2_CLI_0.2.0

└──▷ **BREAKING ON UPGRADE**

! The retired standalone skill-gate script now exits with an error; replace it with `safe2 gate skill PATH --strict`.

! AISM ingestion now rejects ambiguous JSON, unsafe paths, invalid Challenge runs, and existing output files — use a new output filename on each run.

WAS THIS USEFUL?  

garak

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

Garak scans language models and applications for vulnerabilities including prompt injection and data leakage.

> garak v0.17.0 adds EU AI Act risk category mapping for probe results and expands Ollama generator support with authentication, custom clients, and parameter forwarding, while dropping Python 3.10 support.

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

01 **Ollama generator auth and parameter support** IMPROVED 45

The Ollama generator gains authentication and custom client kwargs support, and now forwards generation parameters to Ollama via an options dict.

— Names generator and options dict but no exact flag names v0.17.0

02 **EU AI Act risk mapping for probes** NEW 40

garak now tags and groups probe results by EU AI Act risk categories, mapping scan findings to the corresponding regulatory risk classifications.

— Describes what it does but no config keys or usage shown v0.17.0

03 **Python 3.10 support dropped** BREAKING 35

Python 3.10 is no longer supported by garak; Python 3.13 is now supported.

— Clear version change but no migration guidance v0.17.0

└──▷ **BREAKING ON UPGRADE**

! Python 3.10 is no longer supported; Python 3.13 is now supported.

WAS THIS USEFUL? 👍 👎

AI-Infra-Guard

Feedback

ⓘ

1 RELEASE · 2026-09-10

NOTES ↗

RANK

A full-stack AI Red Teaming platform securing AI ecosystems via Agent Scan, Skills Scan, MCP scan, AI Infra scan and LLM jailbreak evaluation.

> AI-Infra-Guard's v4.6.1 release expands the API Checker's model fingerprinting with support for additional providers.

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

01 **Gemini, Gemma, and GLM fingerprints in API Checker** IMPROVED

41

The API Checker now identifies Gemini, Gemma, and GLM models via new fingerprints, and updates the GLM-5.3-Flash fingerprint baseline.

— Names specific model fingerprints but no mechanism detail v4.6.1

WAS THIS USEFUL? 👍 👎

Certiv

Feedback ⓘ 1 RELEASE · 2026-09-04 BLOG ↗ RANK

Complete visibility and control over every AI agent locally installed on the endpoint. Discover, understand, and safeguard every AI action across your organization.

> Certiv introduced Certiv Cost in public preview, giving organizations session-level token cost attribution plus per-endpoint budget enforcement and a self-service usage view for end users.

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

01 **Per-endpoint budget enforcement in Certiv Cost** NEW

83

Adds per-endpoint dollar budgets with three enforcement modes — Report, Notify, and Block — where Block stops prompts at the endpoint before they are sent. Supports configurable custom rates per model so thresholds reflect negotiated pricing rather than list pricing, and includes a budget simulation feature that shows how often an endpoint would have hit a proposed threshold using historical usage, to help calibrate limits before enforcing them.

— Names exact enforcement modes and mechanism but lacks config path or command

launch-20260904-934ae61c

THINNER COVERAGE BELOW

02 **Scout view for end-user token usage** NEW

50

Adds a Scout view giving end users visibility into their own per-endpoint token consumption broken out by hour, without requiring administrator access.

— Names the feature and behavior but no exact navigation or config given

launch-20260904-934ae61c

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

kubernetes-helm

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

RANK

The Kubernetes Package Manager

> Helm's v4.3.0 release (mirrored in accompanying docs) focuses on rollback auditability and reproducible builds, adding a documented rollback reason, revision tracing in history, duration template functions, `SOURCE_DATE_EPOCH` support, ownership checks before uninstall, and faster status computation for large releases.

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

01 Rollback description and history tracing NEW

85

`helm rollback` gains a `--description` flag to record a human-readable reason for the rollback (max 256 characters) in the release history, and `helm history` output now adds a rollback revision column so operators can trace which revision triggered each rollback.

Document why a rollback was performed so the reason is visible in audit history.

```
$ helm rollback my-release 3 --description 'Reverting due to latency spike in v4 deployment'
```

Roll back a release and capture the reason in release history for audit trails.

```
$ helm rollback my-release 2 --description 'Reverting due to latency regression in v1.4.2'
```

— Names exact flag, character limit, and new history column v4.3.0

02 Reproducible chart archives via SOURCE_DATE_EPOCH NEW

80

`helm package` now honors the `SOURCE_DATE_EPOCH` environment variable when producing chart archives, enabling reproducible, deterministic builds for CI pipelines and supply-chain verification.

Produce a reproducible chart archive with a fixed modification timestamp for deterministic CI builds.

```
$ SOURCE_DATE_EPOCH=1700000000 helm package ./mychart
```

Produce a reproducible chart archive tied to a specific timestamp for supply-chain verification.

```
$ SOURCE_DATE_EPOCH=1700000000 helm package ./my-chart
```

— Names exact env var with a runnable command example v4.3.0

THINNER COVERAGE BELOW

03 **Ownership verification before uninstall deletion** NEW

50

Helm now performs ownership verification before deleting resources during `helm uninstall`, preventing accidental removal of resources that are not owned by the release.

— Explains mechanism but gives no command or flag v4.3.0

04 **Debug logging for empty lookup results** IMPROVED

40

The template engine now emits debug logging when the `lookup` function returns empty results, aiding troubleshooting of missing lookups in chart templates.

— Describes behavior but no log format or example shown product docs

05 **Concurrent status computation for large releases** IMPROVED

35

Helm enables concurrent status computation to prevent multi-minute delays on releases with many resources.

— States the benefit but no numbers or flags given v4.3.0

06 **Duration functions in chart templates** NEW

30

Adds duration template functions to the Helm chart templating engine for time-based calculations in charts.

— Names the capability but no function names or usage v4.3.0

WAS THIS USEFUL? 👍 👎

Microsoft code-oss

Feedback ⓘ 1 RELEASE · SEEN 2026-09-10

BLOG ↗ RANK

Visual Studio Code

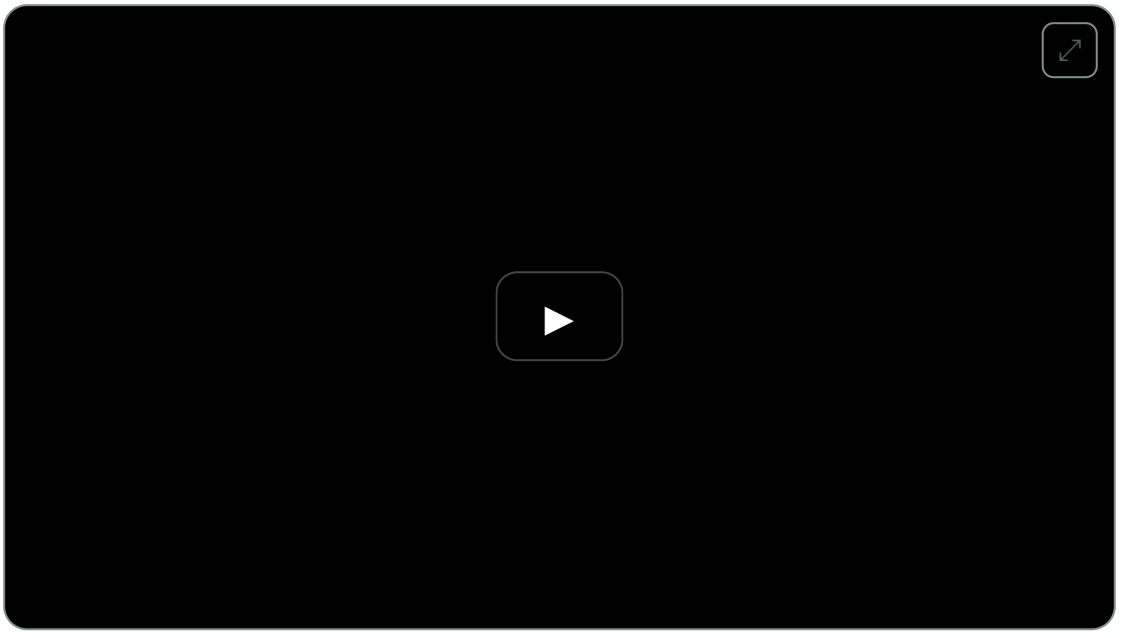
> VS Code introduces the Agent Host and an open Agent Host Protocol (AHP) for persistent, multi-client agent sessions, alongside a major expansion of the Agents window spanning layered approvals and sandboxing, harness handoff, Cloud PR-based delegation, scheduled Automations, and Git worktree isolation.

└──▷ **WHAT SHIPPED · 17 FEATURES** most completely described first ? what's the number?

01 Agent Host process and Agent Host Protocol (AHP) NEW

91

Introduces the Agent Host, a self-contained process that owns agent sessions independently of any editor window so sessions stay alive after closing a folder or window; start one locally with `code agent host` (or `code-insiders agent host` for Insiders). Defines the open Agent Host Protocol (AHP) for coordinating multiple independent clients around the same long-running session via URI-addressable channels (sessions, chats, terminals, changesets), supports multiple agent harnesses (Copilot via GitHub Copilot SDK, Claude via Anthropic Claude Agent SDK) sharing a common AHP session model within one host, and enables remote sessions reachable from desktop, browser (`insiders.vscode.dev/agents`), SSH, or dev tunnels. The new Agents window acts as a synchronized client, letting practitioners monitor and interact with the same live session from an editor window and the Agents window simultaneously.



Start a standalone Agent Host so external AHP clients (or a browser at `insiders.vscode.dev`/agents) can connect to your local sessions without keeping an editor window open.

```
$ code agent host
```

Monitor a running agent session from the browser while the host continues work on your dev machine — navigate to the Agents window in VS Code, connect it to the remote Agent Host, start a session, then open the same host in the browser.

> 📍 Open the Agents window in VS Code › select your remote Agent Host from the host picker › start or open a session › navigate to `insiders.vscode.dev`/agents in your browser › select the same host to continue the session.

— Names CLI command, protocol channels, harnesses, and remote access surfaces.

`launch-20260910-5e9a447f`

02 **Agents window configuration settings** NEW 88

Adds `chat.agentHost.byokModels.enabled` to make Bring Your Own Key models available in Agent Host sessions and `chat.agentHost.allowSignedOutWhenUsable` (experimental) to enable Claude, Codex, and BYOK models in the desktop Agents window without GitHub sign-in. Adds `sessions.layout.singlePaneDetailPanel` for an experimental single-pane layout combining the editor and side panel into one docked pane with a shared tab bar for Changes, Files, Browser, and Search, and `sessions.layout.autoCollapseSessionsSidebar` to auto-hide the sessions sidebar on narrow windows. Adds `extensions.supportAgentsWindow` to opt extensions into the Agents window by extension ID, and supports per-window settings overrides so settings can be scoped to the Agents window without affecting the main editor window.

Opt a specific extension into the Agents window so it activates during agent sessions alongside your main editor.

```json
{
  "extensions.supportAgentsWindow": {
    "myextension.id": true
  }
}
```

Enable the experimental single-pane layout in the Agents window so files and diffs open in a docked editor next to chat instead of a modal.

```json
{
  "sessions.layout.singlePaneDetailPanel": true
}
```

Allow Claude or BYOK models to run in the desktop Agents window without requiring GitHub sign-in.

```json
{
  "chat.agentHost.allowSignedOutWhenUsable": true,
  "chat.agentHost.byokModels.enabled": true
}
```

Use BYOK credentials (e.g. Anthropic or OpenAI) to run Agent Host sessions without signing in to GitHub.

> 📍 In VS Code settings, set `chat.agentHost.byokModels.enabled` to true, then open the Agents window. The model picker will show models from your configured BYOK providers.

— Names six distinct config keys with example JSON snippets. product docs

---

03 **Automations for scheduled agent sessions** NEW 88

Enables `chat.automations.enabled` to unlock an Automations panel in the Agents window sidebar for running saved prompts on a schedule (Manual, Hourly, Daily, or Weekly) against a chosen workspace and agent. Includes a run History view per automation to inspect, stop, or diagnose failures on past sessions before re-running; off by default in VS Code Stable.

Enable Automations in VS Code Stable (off by default) so the Automations panel appears in the Agents sidebar.

> 📍 1. Open the Settings editor (Ctrl+,). 2. Search for `chat.automations.enabled`. 3. Check the box to enable it. 4. Open the Agents window — the Automations entry now appears in the sidebar.

Create a daily automation that summarises the last 24 hours of Git commits and posts a grouped report — useful for async team stand-ups.

> 📍 1. In the Agents sidebar, select Automations › Create Automation. 2. Set Name: Daily commit summary. 3. Set Prompt: 'Summarize commits on the current branch from the last 24 hours. Group by feature, fix, and maintenance work. Include

commit references and flag changes that might need documentation. Do not modify files.' 4. Choose your Git workspace and agent; optionally select `New Worktree` for isolation. 5. Set Schedule to `Manual`, select `Create`, then select `Run now` to verify output under History. 6. Once satisfied, edit the automation, set Schedule to `Daily`, pick a Time, ensure `Enabled` is checked, and select `Save`.

Schedule a nightly code-review automation so the agent runs a saved prompt against your repo every day without manual intervention.

> 📍 In VS Code settings, set `chat.automations.enabled` to true, then open the Agents window and select Automations in the sidebar. Create a new automation, enter your saved prompt, and set the schedule to daily.

— Names the setting, schedule options, and a full walkthrough. `product docs`

---

04 **Sandbox isolation for agent terminal commands** NEW

87

Introduces sandboxing as an independent security layer restricting file system and network access for agent terminal commands regardless of permission level. Adds `chat.agent.sandbox.allowAutoApprove` to require the normal approval flow for sandboxed commands, `chat.agent.sandbox.allowNetworkAccess` to give sandboxed commands unrestricted network access while keeping file system restrictions, `chat.agent.sandbox.networkAccess` as a fallback controlling behavior when network restrictions block a command (default: prompt to retry with unrestricted network), and `chat.agent.sandbox.allowElevation` to stop the agent offering to run a command outside the sandbox when it can't run inside it.

Lock down a high-risk session by keeping the sandbox on but requiring explicit approval for every terminal command inside it — useful when reviewing untrusted code.

> 📍 In the chat input, open the permissions dropdown and select `Manual permissions`, then confirm that `chat.agent.sandbox.enabled` is `true` and `chat.agent.sandbox.allowAutoApprove` is `false` in your workspace settings.

— Names four sandbox settings with defaults and a lockdown example. `product docs`

---

05 **Prompt file and location-settings migration tooling** NEW

86

Adds `chat.customizations.promptMigration.enabled` (default `true`) to control prompt-file-to-skills migration, and `chat.customizations.locationsMigration.enabled` (default `false`) to migrate custom agents, instructions, and skills from folders configured via the deprecated location settings. Surfaces `Migrate Prompt Files` and `Migrate Location Settings` cards in

the Agent Customizations editor when an Agent Host is selected and the corresponding setting is enabled.

Enable location-settings migration so the Agent Customizations editor surfaces the `Migrate Location Settings` card for your Agent Host.

```yaml
chat.customizations.locationsMigration.enabled: true
```

Convert existing workspace prompt files to agent skills so they continue working after the Local agent is removed.

> 📍 1. In the Chat view, select the Agent Host that should use the skills. 2. Open the Agent Customizations editor and select `Migrate Prompt Files`. 3. Choose 'Convert to Skills...' and select the prompt files to convert. 4. In the confirmation dialog, choose whether to delete the original prompt files, then select `Convert to Skills`.

— Names both settings, defaults, and exact migration UI steps. `product docs`

---

06 **Terminal auto-approval rule syntax** NEW 78

Adds per-command terminal auto-approval rules in settings — set a command to `true` to auto-approve or `false` to require approval, wrap patterns in `/` for regex matching, and use the new object syntax with `matchFullCommand` to evaluate the full command line instead of each subcommand individually. Adds `chat.agent.terminalApproval.useOnlyCustomRules` (experimental) to ignore built-in terminal approval rules and rely solely on user-defined ones.

— Names exact rule syntax and setting, no runnable example. `product docs`

---

07 **Cloud target for remote PR-based task delegation** NEW 78

Adds a Cloud target in the Agents window that runs an agent harness on remote infrastructure, implements a task on a branch, and opens a GitHub pull request for review — selected from the harness control alongside your repository, agent role, and permissions.

Delegate a well-scoped coding task to the Cloud target so it runs remotely and opens a pull request — no local editor context needed.

> 📍 In the Agents window: select the Cloud target from the harness control › choose your GitHub repository › configure the agent role and permissions › start the

session. The agent implements the task on a branch and opens a pull request for your review.

— Describes mechanism and gives exact navigation steps. product docs

08 **Session permission levels and tool approval management** NEW

75

Adds a permission level dropdown in the chat input to switch between Manual, AI-judged, and a new session-scoped `Allow all` level that bypasses approvals only for the current local or Copilot CLI session without enabling global auto-approval. Adds `Run 'Configure Tool Approvals'` from the Command Palette to review and set per-tool approval state (auto-approve run, auto-approve result, or always require manual approval) grouped by source, and `Run 'Clear All Tool Approvals'` to reset all saved tool approvals at once.

— Names dropdown levels and two exact command palette commands. product docs

09 **Shell environment setup for local Copilot sessions** NEW

75

Adds `chat.agentHost.shellTool.initScript.enabled` to load `.bashrc` or PowerShell profiles before each command in local Copilot sessions using the SDK built-in shell tool, and sets `python-envs.terminal.autoActivationType` to `shellStartup` to auto-activate the selected workspace Python environment in those sessions.

Enable shell init scripts so your `.bashrc` profile (and activated Python environment) load before each agent command in a local Copilot session.

```json
"chat.agentHost.shellTool.initScript.enabled": true,
"python-envs.terminal.autoActivationType": "shellStartup"
```

— Names both config keys with a runnable settings snippet. product docs

10 **Prompt files and location settings deprecated for Agent Host**

DEPRECATED

70

Prompt files are deprecated for Agent Host sessions and are no longer loaded by Agent Host — they must be converted to agent skills to remain available, and the Local agent will be removed in a future release. The `chat.agentFilesLocations`, `chat.modeFilesLocations`, `chat.instructionsFilesLocations`, and `chat.agentSkillsLocations` settings are deprecated since Agent Host does not read them, and Agent Host sessions now load user-level customizations from supported folders instead of VS Code profile user data and VS Code-specific formats; custom

agents/instructions in profile user data must be migrated to the selected Agent Host's user folders.

— Names deprecated settings and before/after behavior, no direct command. product docs

11 **AHP client libraries in five languages** NEW 65

Publishes official Agent Host Protocol client libraries: Rust (`ahp` , `ahp-types` , `ahp-ws`), TypeScript (`@microsoft/agent-host-protocol`), Kotlin (`com.microsoft.agenthostprotocol:agent-host-protocol`), Go (`github.com/microsoft/agent-host-protocol/clients/go`), and Swift (via Swift Package Manager: `microsoft/agent-host-protocol`).

— Lists exact package names but no usage example given. launch-20260910-5e9a447f

12 **Session handoff between agent harnesses and Codex support** NEW 65

Enables session handoff, carrying conversation history and context when switching harnesses (Copilot, Claude, Codex, or Cloud) mid-task, including a Start Implementation handoff action that moves from a Plan agent to an available implementation agent while preserving context. Codex can now run on the Agent Host, making it available in the Agents window alongside the existing OpenAI extension Codex target.

Hand off an in-progress plan to an implementation agent without losing conversation history.

> 📍 In the Chat view or Agents window: after the Plan agent completes its plan, select Start Implementation › choose an available implementation agent (Copilot, Claude, or Codex). VS Code carries the full conversation history and context to the new agent.

— Names the handoff action and harnesses but limited mechanism detail. product docs

13 **Markdown Editor (Experimental) in Agents window** NEW 62

Adds `workbench.editor.markdownDefaultEditorInAgentsWindow` setting to control whether `.md` files open with the new Markdown Editor (Experimental) or Markdown Preview by default. The experimental editor supports Editing and Locked modes with Git change markers in the margin — green for added, blue for modified, red for deleted.

— Names setting and modes but no walkthrough given. product docs

14 **Git worktree isolation for agent sessions** NEW 60

Adds code isolation via Git worktree so agent file changes stay separate from the active workspace: available in the Agents window via a New Worktree checkbox with base-

branch control, as a New Worktree isolation option for Git workspaces when creating an Automation, and as a worktree isolation mode for workspace sessions generally.

— Explains mechanism across three surfaces, no exact setting name. product docs

THINNER COVERAGE BELOW

15 **Voice Mode, quick chat promotion, and browser preview in Agents window**

NEW 49

Adds Voice Mode to the Agents window chat input for steering active sessions by speech, the ability to promote a quick chat into a full workspace session while preserving title, conversation history, and the in-flight request, and a per-session browser preview panel accessible via right-click in the file explorer or a terminal link so agents can inspect and interact with web applications.

— Three distinct additions each described only briefly. product docs

16 **Two-step URL approval for agent requests** NEW 47

Separates request approval (via the Trusted Domains list) from response approval for URLs an agent fetches, preventing data exfiltration and prompt injection independently.

— Explains mechanism but no setting name or steps. product docs

17 **Advanced Autopilot mode** NEW 28

Introduces Advanced Autopilot mode, which delegates turn-completion decisions to a secondary model; enabled via a dedicated preview setting.

— No named setting or configuration given. product docs

└──▷ **BREAKING ON UPGRADE**

! Prompt files are deprecated for Agent Host sessions and are not loaded by Agent Host; they must be converted to agent skills to remain available (the Local agent will be removed in a future release).

! The `chat.agentFilesLocations`, `chat.modeFilesLocations`, `chat.instructionsFilesLocations`, and `chat.agentSkillsLocations` settings are deprecated because Agent Host sessions do not use them.

! Custom agents and instructions stored in VS Code profile user data are not read by Agent Host; they must be migrated to the user folders for the selected Agent Host.

WAS THIS USEFUL? 👍 👎

OpenSSL

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

General purpose TLS and crypto library

> OpenSSL 4.1 lands full DTLS 1.3 (RFC 9147) support with a new listener API and post-quantum crypto over DTLS, alongside RFC 8701 GREASE support, new architecture and build-target support, several PQC/AES performance optimizations, and a handful of breaking removals in build targets, Configure options and the tsget utility.

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

01 DTLS 1.3 protocol support NEW

88

OpenSSL 4.1 adds full DTLS 1.3 (RFC 9147) support, documented in the ossl-guide-dtlsv13(7) manual page, with fewer handshake round trips and removal of outdated cryptographic algorithms compared to DTLS 1.2. SSL_new_listener() is extended to support DTLS, enabling DTLS 1.3 listener workflows (note DTLSv1_listen() does not support DTLS 1.3), and Post-Quantum Cryptography algorithms — building on the PQC foundation introduced in OpenSSL 3.5 — now work over DTLS 1.3. Reference demos `demos/dtlsecho` and `demos/dtlslistenerecho` illustrate client/server usage.

Consult the new DTLS 1.3 guide to understand how to establish DTLS 1.3 connections using the updated API.

```
$ man ossl-guide-dtlsv13
```

— Named API, man page and demo paths with clear mechanism launch-20260909-6052d4b0 launch-20260909-33f13a94

02 tsget now requires Net::Curl::Easy BREAKING

70

The `tsget` utility now requires `Net::Curl::Easy` (from the Net-Curl CPAN distribution) instead of the abandoned `WWW::Curl::Easy` — install `Net::Curl::Easy` before upgrading.

— Exact dependency swap with clear upgrade action launch-20260909-33f13a94

03 Removed legacy build targets and Configure flags BREAKING

60

Windows-on-Itanium (`VC-WIN64I`) and Windows CE (`VC-CE`) build targets have been removed from Configurations. The `no-ecdsa` and `no-ecdh` options have been removed from Configure ; use `no-ec` to disable elliptic curve support.

— Names removed flags and the replacement option launch-20260909-33f13a94

THINNER COVERAGE BELOW

04 **PQC and AES performance optimizations** IMPROVED 58

Adds AVX-512-optimized SHAKE x4 operations for ML-DSA on x86_64, AVX-512 and VAES optimizations for AES-CBC decryption on x86_64, optimized ML-DSA and ML-KEM NTT operations on ppc64le, and optimized ML-DSA operations on s390x and x86_64.

— Names algorithms and architectures but no benchmarks launch-20260909-33f13a94

05 **MSVC 2013 build targets** NEW 50

Adds `VC-WIN32-MSVC2013` and `VC-WIN64A-MSVC2013` build targets to bridge C99 support gaps in MSVC 2013.

— Names exact build targets, minimal further detail launch-20260909-33f13a94

06 **GREASE extension support in TLS** NEW 35

Adds support for RFC 8701 GREASE (Generate Random Extensions And Sustain Extensibility) in TLS.

— Names the RFC but no config or API surface given launch-20260909-33f13a94

07 **Elbrus2000 (e2k) architecture support** NEW 18

Adds initial support for the Elbrus2000 (`e2k`) architecture.

— Bare name, no detail on scope or usage launch-20260909-33f13a94

└──▷ BREAKING ON UPGRADE

! The `tsget` utility now requires `Net::Curl::Easy` (from the Net-Curl CPAN distribution) instead of the abandoned `WWW::Curl::Easy` — install `Net::Curl::Easy` before upgrading.

! Windows-on-Itanium (`VC-WIN64I`) and Windows CE (`VC-CE`) build targets have been removed from Configurations.

! The `no-ecdsa` and `no-ecdh` options have been removed from `Configure` ; use `no-ec` to disable elliptic curve support.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 10, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue