THE CYBER TOOLCHAIN

NO. 098

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED OCTOBER 9, 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 29 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 12 tools

▾ // THE BRIEF HIDE

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

DETECT

Kill a process from a kernel detection rule instead of shipping the
nt and waiting

vim ? help

Kunai 0.6.0's rule engine supports kill and Yara-scan actions, rule composition via dependencies, and IoC-file matching against hashes, paths, domains and IPs, over 30+ documented kernel event types. The loop from eBPF event to response collapses onto the host, rather than round-tripping through a SIEM that sees the execve minutes after it mattered.

Kunai

PROTECT

Scan an API for XSS from its own spec, and tune out the noise before triage

Dalfox ingests OpenAPI, Swagger and Postman definitions as target sources and adds `--min-confidence` filtering across CLI, config, REST API, MCP and SARIF, so low-confidence hits never reach the queue. Noir separately disables curl URL globbing by default, which stops path parameters containing braces and brackets being mangled in generated requests.

Dalfox · noir

DETECT

Tie a packet to the process that sent it, on the same pane

4.7.5 records per-packet process metadata and can strip it before sharing a capture. Attributing suspicious traffic to a binary normally means correlating a capture against separate endpoint telemetry by timestamp and port; this puts the answer in the packet detail, and the strip option keeps host names and PIDs out of a capture handed to a third party.

Wireshark

PROTECT

Hand DNS filtering to a team that is not domain admin

Twingate's Internet Security role scopes DNS filtering and Exit Network management without full admin rights — the standing argument against delegating web filtering is that the only role that can do it can also rewrite network policy. Okta's 2026.41.0 promotes OAuth 2.0 On-Behalf-Of token exchange with actor claim stamping to GA, so a delegated service call carries a verifiable record of who acted on whose behalf.

Twingate · Okta Identity Engine

APPLICATION SECURITY

◆ Secrets Detection & Management

infisical

Feedback ⓘ v0.166.3 NOTES ↗

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

Adds Ed25519 KMS sign/verify keys, GCP service account key rotation, multi-connection secret rotation, and a pre-sync path warning.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.166.3
https://github.com/Infisical/infisical.git
# already have the repo? check out this version:
$ git checkout v0.166.3
```

Adds Ed25519 sign/verify key support in KMS, enabling elliptic-curve signing operations.

Adds GCP service account key rotation to the secret rotation engine.

Adds support for multiple connections in a single secret rotation configuration.

Warns users before moving or copying secrets into a synced path, preventing unintended sync overwrites.

NEW INTEGRATION UltraDNS ACME DNS-01 provider

NEW INTEGRATION Google Cloud DNS ACME DNS-01 provider

NEW INTEGRATION HPE iLO Redfish app connection

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

GitHub

Feedback ⓘ

Triage role users or higher can now archive pull requests (2026-10-08) BLOG ↗

RANK

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

> GitHub extended pull request archiving to triage-role users and made archived PRs fully read-only for everyone, including admins.

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

01 Expanded PR archiving permissions and read-only enforcement

70

BREAKING

Users with the triage, write, maintain, or admin role can now archive and unarchive pull requests, a capability previously limited to admins. Once archived, a PR's conversation becomes fully read-only — new comments, reactions, and automated comments are blocked for all users including admins — and archived PRs are hidden from public view but remain visible to repository administrators. This changes prior behavior where admins could still comment on a locked/archived PR.

Triagers handling spam or abandoned PRs can now archive them directly in the UI without escalating to an admin.

> 📍 In the pull request page, open the pull request actions menu and select `Archive pull request`. The PR will be closed and its conversation made read-only immediately.

– Clear before/after and UI steps, no API/flag named

Triage role users or higher can now arc…

└──▷ BREAKING ON UPGRADE

! Archiving a pull request now blocks all new activity (comments, reactions, automated comments) for every role including admins — previously admins could still comment on a locked/archived PR.

WAS THIS USEFUL? 👍 👎

Cisco skill-scanner

Feedback ⓘ 2.2.2 NOTES ↗ CODE ↗

RANK

The skill-scanner is a security scanner for AI agent skills

> Skill Scanner 2.2.2 adds a new detection rule for whole-environment variable dumps and introduces separate controls over the adjudicator LLM's output length and reasoning mode, the latter arriving disabled by default as a breaking change.

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

01 **Adjudicator reasoning effort control, disabled by default**

62

BREAKING

Adds `SKILL_SCANNER_ADJUDICATOR_LLM_REASONING_EFFORT` environment variable to override the adjudicator's reasoning mode. As of this release the adjudicator's reasoning is now disabled by default; set this environment variable to restore the previous behaviour.

– Exact env var and before/after default behaviour stated 2.2.2

THINNER COVERAGE BELOW

02 **Whole-environment dump detection rule** NEW

57

Adds a `DATA_EXFIL_ENV_DUMP` detection rule that flags whole process-environment value dumps in Python, JavaScript/TypeScript, and shell code, covering targeted reads, keys-only enumeration, literal examples, and comments, with severity kept below the HIGH rule boundary.

– Names rule and languages covered but no usage example 2.2.2

03 **Adjudicator LLM max output tokens control** NEW

50

Adds `SKILL_SCANNER_ADJUDICATOR_LLM_MAX_TOKENS` environment variable to set a separate output-token limit for the adjudicator LLM.

– Exact env var name given, no further mechanism detail 2.2.2

04 **Shell prompt and command must share a line** BREAKING

40

A shell prompt marker by itself no longer captures a command on the next line; the prompt and command must now share a single line for the parser to associate them.

– States behaviour change but no migration example 2.2.2

└──▷ BREAKING ON UPGRADE

! The adjudicator's reasoning is now disabled by default; set `SKILL_SCANNER_ADJUDICATOR_LLM_REASONING_EFFORT` to restore the previous behaviour.

! A shell prompt marker by itself no longer captures a command on the next line; prompt and command must share a line.

WAS THIS USEFUL?  

Veracode

Feedback ⓘ Integration updates (2026-10-08) BLOG ↗

Veracode is a cloud-based application security platform that performs static, dynamic, and software composition analysis to identify vulnerabilities in code.

Veracode integrations add IaC policy enforcement, pre-dependency commands, Git scan metadata, platform-level GitHub install/schedule management, and expanded VS Code and JetBrains IDE filtering.

Adds `policy` parameter to `veracode.yml` in the Azure DevOps, GitLab, and GitHub Workflow Integrations for infrastructure-as-code (IaC) scans.

Adds `predependency_command` parameter to `veracode.yml` in the GitLab and Azure DevOps Workflow Integrations to run commands before Veracode packages the project.

Java API wrapper v26.10.20.0 automatically includes Git repository and commit metadata (branch, commit, author, repository, and Git provider) in Static Analysis scans for JAR, WAR, EAR, and ZIP archives.

NEW INTEGRATION GitHub Workflow Integration v2.0.0 enables installing, configuring, and scheduling Static Analysis, SCA, and IaC scans directly from the Veracode Platform.

GitHub Workflow Integration adds a new uninstallation workflow on the Veracode Platform.

+3 more

NEW SUPPORTED PLATFORM JetBrains IDE versions 2024.2 through 2026.3

NEW SUPPORTED PLATFORM Jira 11 support in Veracode Integration for Jira Server

RETIRED SUPPORTED PLATFORM End of support for Jira 9 in Veracode Integration for Jira

NEW INTEGRATION Autopackaging support for Apex, VB6, and Perl in GitHub Workflow Integration

└──▷ BREAKING ON UPGRADE

! Veracode Azure DevOps Extension v4.0.0 deprecates Veracode Flaw Importer v3 and replaces it with VeracodeFlawImporter v4; existing pipelines must be manually migrated from v3 to v4.

WAS THIS USEFUL? 👍 👎

◆ OT / ICS Security

cisagov CSET

Feedback ⓘ v13.0.0.0 NOTES ↗

Cybersecurity Evaluation Tool

CSET v13 adds light/dark mode, a redesigned grid-based assessment gallery with favoriting, an improved My Assessments grid, and a persistent completion-tracking header.

└──▷ GET THIS VERSION

```
$ git clone --branch v13.0.0.0 https://github.com/cisagov/cset.git
# already have the repo? check out this version:
$ git checkout v13.0.0.0
```

Adds light and dark theme support throughout the UI.

Redesigns the assessment gallery from sideways-scrolling card rows to a full grid layout per category, with favoriting for quick access.

Improves the My Assessments grid with resizing, paging, filtering, sorting, and favoriting.

Adds a persistent assessment header that stays visible while working through an assessment and shows completion progress.

NEW COMPLIANCE FRAMEWORK CPG v2.0 (Cross-Sector Cybersecurity Performance Goals)

NEW COMPLIANCE FRAMEWORK EVCI Assessment (EV Charging Infrastructure Assessment & Evaluation)

UPDATED COMPLIANCE FRAMEWORK NIST SP 800-53 updated to Revision 5.2.0

UPDATED COMPLIANCE FRAMEWORK NIST SP 800-171 updated to Revision 3

UPDATED COMPLIANCE FRAMEWORK NIST SP 800-161 updated to Revision 1

UPDATED COMPLIANCE FRAMEWORK AWWA updated to version 4.0

UPDATED COMPLIANCE FRAMEWORK PCIDSS updated to version 4.0.1

RETIRED COMPLIANCE FRAMEWORK Retired CISA-sponsored assessment types

└──▷ BREAKING ON UPGRADE

! New assessments of the following retired types can no longer be created after upgrading to v13.0: Cyber Resilience Review (CRR), External Dependencies Management (EDM), Incident Management Review (IMR), Ransomware Readiness

Assessment (RRA), Cyber Infrastructure Survey (CIS), and Cross-Sector Cybersecurity Performance Goals (CPG) v1.0.1.

WAS THIS USEFUL? 👍 👎

cisagov Malcolm

Feedback ⓘ v26.09.0 NOTES ↗ RANK

Malcolm is a powerful, easily deployable network traffic analysis tool suite for full packet capture artifacts (PCAP files), Zeek logs and Suricata alerts.

> Malcolm v26.09.0 adds configurable Suricata rule-update scheduling, raw compressed-PCAP uploads, an early MITRE OTKB enrichment integration, a configurable default landing dashboard, and NetBox refinements for subnet autopopulation and IP enrichment.

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

01 **Configurable Suricata rule-update schedule** NEW 86

Adds `SURICATA_UPDATE_CRON_EXPRESSION` to make the Suricata rule-update schedule configurable, `SURICATA_UPDATE_RULES=true` to trigger a rule update at container startup, `SURICATA_UPDATE_ENABLE_SOURCES` to enable indexed `suricata-update` sources (e.g., `et/pro`) with optional parameters, and `SURICATA_UPDATE_SOURCES` to expose the source-index refresh toggle — all set in `config/suricata.env`.

Schedule Suricata rule updates to run nightly at 02:00 and also pull updates once at container startup, with a commercial ET/Pro source enabled.

ini

```
SURICATA_UPDATE_CRON_EXPRESSION='0 2 * * *'
SURICATA_UPDATE_RULES=true
SURICATA_UPDATE_ENABLE_SOURCES='et/pro secret=<your-oinkcode>'
SURICATA_UPDATE_SOURCES=true
```

— Four named env vars with exact file and runnable example. v26.09.0

02 **MITRE OTKB enrichment integration** NEW 78

Adds an optional early integration with MITRE's Operational Technology Knowledge Base (OTKB), enriching supported Zeek and Wireshark OT events with normalized protocol, function, classification, citation, procedure, asset, campaign, software, and MITRE ATT&CK for ICS context under a new `otkb.*` field hierarchy, including an OpenSearch composable template and an OT Knowledge Base dashboard, with support for connected, air-gapped, and file-seeded-then-API-refreshed deployments.

— Rich mechanism and field schema, but no exact config shown. v26.09.0

03 **Configurable default landing dashboard** NEW 65

Adds `OPENSEARCH_DEFAULT_DASHBOARD` to the `dashboards-helper.env` configuration template, letting operators pin the landing dashboard to one of four named

options: Overview, Security Overview, ICS/IoT Security Overview, or Severity.

Pin the Malcolm landing page to the ICS/IoT Security Overview dashboard for OT-focused deployments.

```ini
OPENSEARCH_DEFAULT_DASHBOARD=ICS/IoT Security Overview
```

— Named config key, file, and four options with example value. v26.09.0

04 **NetBox autopopulation for public subnets** NEW 65

Adds `NETBOX_AUTO_POPULATE_SUBNETS` to allow NetBox autopopulation to include explicitly listed public IP subnets, with private-only remaining the default when the variable is blank.

Allow NetBox autopopulation to enrich events from a known public sensor subnet in addition to RFC-1918 space.

```ini
NETBOX_AUTO_POPULATE_SUBNETS='203.0.113.0/24'
```

— Named env var, file, and default behavior with example. v26.09.0

05 **Compressed PCAP upload support** NEW 60

Adds support for uploading raw gzip-, bzip2-, xz-, and lzma-compressed PCAP/PCAPNG files; the upload watcher decompresses the stream with libmagic and routes recognized PCAP content to the PCAP processing directory, while non-PCAP compressed streams and tar archives continue through the existing path.

— Mechanism explained but no exact command to invoke it. v26.09.0

THINNER COVERAGE BELOW

06 **Longest-prefix-match NetBox IP enrichment** IMPROVED 55

Improves NetBox IP enrichment to prefer the most specific (longest-prefix-match) prefix, preventing parent and child prefixes from both being applied and producing multi-valued `source.segment` / `destination.segment` fields.

— Explains behavior fix but is automatic, no config to act on. v26.09.0

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Corellium

Feedback ⓘ Release 7.14.0 (2026-10-08) BLOG ↗

Advice, answers, updates, and more from the Corellium Team

Corellium 7.14 ships a cluster-hosted MCP server for zero-setup AI agent access, makes Mirror a purchasable Falcon add-on for UFED-based forensic review, and rebuilds API docs on Scalar.

Adds cluster-hosted Corellium MCP server — cloud customers get AI agent access immediately on login with no setup; self-hosted (SA/DA) customers get it bundled with their existing deployment, using existing Corellium credentials with full tenant isolation.

Adds rate limiter on the MCP server keyed by authenticated caller rather than proxy address, and credential redaction from default conversational MCP results.

Adds support for larger HTTP file uploads via the MCP server.

Moves API docs from `/api/docs` to a new UI built on Scalar, with ongoing investigation into surfacing SDK method names and per-language type signatures.

Makes Mirror available as a purchasable add-on to Falcon Essentials or Falcon Premium — loads a Cellebrite UFED (UFD) extraction directly into a new Corellium iOS virtual device for native app-based review.

NEW SUPPORTED PLATFORM iPhone 18 device support

NEW SUPPORTED PLATFORM iOS/iPadOS 27.x support

NEW SUPPORTED PLATFORM iOS/iPadOS 26.x support

NEW SUPPORTED PLATFORM iOS/iPadOS 18.7.10 support

UPDATED INTEGRATION Frida framework integration updated to 17.19.0 (iOS) and 17.18.0 (Android)

WAS THIS USEFUL? 👍 👎

Trend Vision One

Feedback ⓘ

Dark/light mode is available (2026-10-06) 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 dark/light mode toggle to the console and migrates the Azure Activity Log pipeline to a new event-driven architecture.

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

01 **Dark/light mode toggle in Preferences** NEW 65

A dark/light mode toggle is now available in the Preferences menu, accessible via the user icon at the top right of the console. The selection is saved per account automatically, with dark mode as the default.

Switch the console to light mode when working in bright environments.

> 📍 1. Click your user icon at the top right of the console. 2. Select Preferences. 3. Toggle the display to light mode. 4. Your selection is saved to your account automatically.

— Exact UI navigation steps given, but limited mechanism beyond toggle.

Dark/light mode is available (2026-10-0…

THINNER COVERAGE BELOW

02 **Azure Activity Log pipeline migrated to v2** IMPROVED 30

Azure Activity Log version 1.0.48 migrates its AML pipeline to v2, adopting an event-driven architecture for improved performance and scalability.

— Names version and architecture shift but no concrete metrics or steps.

Azure Activity Log version 1.0.48 (2026…

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Censys

Feedback ⓘ October 8, 2026 (2026-10-08) BLOG ↗ RANK

Censys is a search engine for internet-connected devices that indexes certificates, websites, and network services for security research and reconnaissance.

> Censys shipped AI Investigations for automated threat-hunting pivots and added service account support for machine-to-machine access to the Platform APIs.

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

01 **AI Investigations for threat hunting** NEW 55

A new AI-powered investigator analyzes indicators, pivots to related infrastructure, profiles web resources, checks entity history, and produces a ranked, formatted findings report. It is accessible from the threat-hunting page.

— Describes behavior and entry point but no API or limits product docs

NEW DETECTION Software fingerprints for jQuery, AngularJS, Bootstrap, WordPress, WooCommerce, Astro, and more

October 8, 2026 (2026-10-08) BLOG ↗ LATEST STABLE

Censys ASM adds screenshots, redirect chain analysis, and DOM network logs for web entities, plus CVE risk acceptance on hosts and web assets.

Adds screenshots for every web entity in inventory, captured at scan time and timestamped by Last Updated, enabling rapid identification of exposed login pages, admin panels, and compromised infrastructure.

Adds full redirect chain visibility on web entities to detect domain takeovers or incorrect redirect destinations.

Adds network log view on web entities listing all resources loaded during a full DOM evaluation, including JS libraries, scripts, images, and stylesheets.

Adds ability to accept CVE risk instances on host and web entity assets, accepting all CVE risks associated with a given risk instance at once.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Identity & Access Management

Okta Identity Engine

Feedback ⓘ

Version 2026.41.0 (2026-10-07) BLOG ↗ RANK

Secure, scalable, and highly available authentication and user management for any app.

> Okta Identity Engine's 2026.41.0 release headlines with GA promotions for OAuth 2.0 On-Behalf-Of Token Exchange actor claim stamping and a resource collections API, alongside new NFC authenticator support, Access Certification campaign staging audit events, SCIM password-provisioning controls, and app branding migration tooling, plus a batch of smaller features reaching GA or EA status.

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

01 Access Certification campaign staging System Log events NEW

88

Two new System Log event types track Access Certification campaign staging: `certification.campaign.stage.start` (logged when staging begins) and `certification.campaign.stage.end` (logged when staging ends, with `outcome.result` reporting `SUCCESS` or `FAILURE`). The feature shipped as EA and can be monitored via the System Log API or Admin Console Reports.

Monitor Access Certification campaign staging outcomes in real time by filtering System Log for the new staging events.

```
$ curl -s -X GET 'https://<your-okta-domain>/api/v1/logs?
filter=eventType+eq+"certification.campaign.stage.end"' -H
'Authorization: SSWS <api_token>' -H 'Accept: application/json'
```

Monitor Access Certification campaign staging outcomes in the System Log to detect snapshot failures before a campaign goes live.

📍 In the Okta Admin Console, go to Reports › System Log and filter for event types `certification.campaign.stage.start` and `certification.campaign.stage.end`, then check the `outcome.result` field for `SUCCESS` or `FAILURE`.

— Named events and fields with both API and console usage examples

Version 2026.41.0 (2026-10-07)

02 **Actor claim stamping for OAuth 2.0 On-Behalf-Of Token Exchange**

NEW 78

Access tokens issued via OAuth 2.0 On-Behalf-Of Token Exchange now get an `act` actor claim identifying the requesting service app, with nested `act.act` claims to represent chained delegation. This capability reached GA in Preview.

Inspect the actor claim chain on an On-Behalf-Of access token to verify which service apps participated in the delegation.

> 📍 Decode the issued access token JWT and look for the top-level `act` claim (identifying the immediate requesting service app) and the nested `act.act` claim (identifying the prior delegator in the chain).

— Claim names given plus a concrete JWT inspection step Version 2026.41.0 (2026-10-07)

---

03 **Configurable password provisioning in SCIM user creation** NEW

75

A Set password when creating a new user toggle was added under `Provisioning > To App > Create Users` in SCIM 2.0 test app templates (OAuth Bearer Token, Basic Auth, and Header Auth), letting admins enable or disable password provisioning at user creation; this configurable password provisioning during user creation is now GA.

Disable automatic password provisioning when creating users via a SCIM 2.0 app integration.

> 📍 In the Okta Admin Console, navigate to the SCIM 2.0 app › Provisioning › To App › Create Users, then toggle off 'Set password when creating a new user'.

— Exact UI path and toggle name with console steps given Version 2026.41.0 (2026-10-07)

---

04 **Resource collections API GA in Preview** IMPROVED 63

The resource collections API is promoted to GA in Preview, supporting Okta groups, Okta push groups, and non-Entitlement Management apps without requiring an opt-in to Entitlement Management, and enabling direct assignment of a collection to a principal user.

— Scope and support matrix named but no endpoint or command given product docs

THINNER COVERAGE BELOW

05 **App branding migration for Identity Engine** NEW 50

Eligible orgs can stage, preview, and deploy Identity Engine on a per-app basis while preserving Classic Engine customizations, with per-app rollback if needed.

— Describes mechanism and rollback but no UI path or config

Version 2026.41.0 (2026-10-07)

06 **session.idp property in Okta Expression Language** NEW

45

Adds a `session.idp` property to Okta Expression Language for use in policy and rule expressions that reference the session identity provider.

– Names the property but no example expression Version 2026.41.0 (2026-10-07)

07 **NFC authenticator support for Adaptive MFA** NEW

35

Adds NFC authenticator support for Adaptive MFA, enabling tap-based hardware token authentication flows.

– Describes what it does but no setup detail Version 2026.41.0 (2026-10-07)

08 **WebAuthn enrollments include transports values** IMPROVED

35

WebAuthn authenticator enrollments now include `transports` values, reaching GA in Production.

– Names the field but no usage example Version 2026.41.0 (2026-10-07)

09 **PowerShell scripts for Active Directory reach GA** IMPROVED

27

PowerShell scripts for Active Directory are now GA in Production.

– Bare status change with no script details Version 2026.41.0 (2026-10-07)

10 **Self-service registration policy for ITP** NEW

27

Self-service registration policy for ITP is now self-service EA in Preview.

– Bare status note with no configuration detail Version 2026.41.0 (2026-10-07)

11 **Email channel for Direct Authentication** NEW

27

Email channel for Direct Authentication is now self-service EA in Preview.

– Bare status note with no configuration detail Version 2026.41.0 (2026-10-07)

12 **Passkey enrollment prompt reaches GA** IMPROVED

25

The feature prompting users to enroll a passkey is now GA in Production.

– Bare status change with no mechanism detail Version 2026.41.0 (2026-10-07)

13 **User identification policy reaches GA** IMPROVED

25

User identification policy is now GA in Production.

– Bare status change with no mechanism detail Version 2026.41.0 (2026-10-07)

14 **Single Certificate Issuer reaches GA in Preview** IMPROVED

25

Single Certificate Issuer is now GA in Preview.

— Bare status change with no mechanism detail Version 2026.41.0 (2026-10-07)

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

Twingate

Feedback ⓘ Internet Security role NOTES ↗ RANK

Identity-based access for users, services, and AI agents that deploys in minutes, scales to every resource, and finally lets you retire your VPN.

> Twingate introduces an Internet Security role, letting admins delegate DNS filtering and Exit Network management without granting full admin access.

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

01 **Internet Security admin role** NEW

50

A new Internet Security role lets admins delegate DNS filtering and Exit Network management, Internet Security analytics, and report creation to users without granting them full administrative access.

— Names the role and its scope but no setup steps or UI path. Internet Security role

WAS THIS USEFUL? 👍 👎

AGENT

◆ MCP Servers & Tooling

Runlayer

Feedback ⓘ 1.28.1115 (2026-10-09) BLOG ↗

Runlayer is an MCP gateway that enforces identity-mapped permissions and detects threats across the agents and MCP servers employees use.

Adds artifact folders, agent inventory tab, per-user hook daemon, custom model pricing, Claude Haiku 5.5 support, and richer audit-log policy attribution.

Adds `folder` option on `create_artifact` and the new `set_artifact_folder` tool so agents can file published artifacts into nested folder paths using `/` as a separator.

Adds `aiwatch daemon status` shell command to check whether the per-user hook daemon is running on enrolled macOS and Windows devices.

Adds an Inventory tab on the Agents page listing every editable agent with owner, model, recent runs, and upkeep issues (idle, never run, newer model available, owner left), with bulk model-upgrade and bulk-disable actions; replaces the Unused tab.

Adds per-custom-model input, output, cache-read, and cache-write price configuration under Settings → AI Providers so agent-run cost and budget limits price custom models correctly.

Adds Claude Haiku 5.5 as a selectable agent model via the Anthropic API or AWS Bedrock, with adaptive thinking effort settings.

+6 more

NEW DETECTION Grok Bot desktop app detection (xAI)

NEW DETECTION Meta Muse desktop app detection (macOS)

NEW DETECTION Meta Muse Code terminal agent scanning

UPDATED DETECTION ChatGPT desktop app version reporting on Windows

NEW DETECTION Muse web app (muse.ai) session detection via browser extension

RETIRED DETECTION Legacy macOS Detect script-based agent (com.runlayer.scan) retired by installer

└──▷ BREAKING ON UPGRADE

! The `workspace` built-in MCP server is no longer trusted by default for Claude Code and is removed from existing custom allowed lists; add it back explicitly only if your policy accepts it.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · October 9, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue