THE CYBER TOOLCHAIN

NO. 015

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED JULY 14, 2026 · EVERY WEEKDAY

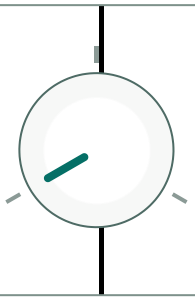
The daily firehose — everything the toolchain shipped today, already filtered.

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 49 tools

OFFENSIVE SECURITY

◆ Post-Exploitation

ligolo-ng ⓘ v0.9 NOTES ↗

An advanced, yet simple, tunneling/pivoting tool that uses a TUN interface.

Ligolo-ng v0.9 adds faster UDP scanning via ICMP, configurable paths, in-flight TCP tuning, cert fingerprint verification, and ARM64 builds.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.9 https://github.com/nicocha30/ligolo-ng.git
# already have the repo? check out this version:
$ git checkout v0.9
```

- Speeds up UDP port scanning by processing ICMP port-unreachable messages to immediately mark closed ports.
- Adds configurable paths for the config file, session history, and self-signed certificates.
- Supports configurable in-flight TCP connection limits for tuning tunnel throughput.
- Enables bind certificate fingerprint verification to authenticate relay/proxy identity.
- Ships ARM64 binaries by default.

WAS THIS USEFUL? 👍 👎

◆ Reconnaissance & OSINT

Maigret ⓘ v0.6.3 NOTES ↗ CODE ↗

Collect a dossier on a person by username from 3000+ sites

Maigret v0.6.3 adds 15 new sites and a DiscourseJson detection engine to its 3,000+ site database.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.6.3 https://github.com/soxoj/maigret.git
# already have the repo? check out this version:
$ git checkout v0.6.3
```

- Adds 15 new sites to the username-search database (two separate batches of 10 and 5).
- Adds support for a new DiscourseJson detection engine, broadening coverage of Discourse-based community forums.
- Adds Chinese-language platforms — including Tuchong, GitCode, Yuque, LeetCode CN, Bangumi, NGA, and Moegirl — to the site database.

WAS THIS USEFUL? 👍 👎

◆ Wireless & RF

airgeddon ⓘ v12.01 NOTES ↗

This is a multi-use bash script for Linux systems to audit wireless networks.

airgeddon v12.01 adds WPA3 MFP analysis, dynamic WPA3 plugin menus, and band-aware WPS/Evil Twin controls.

└──▷ GET THIS VERSION

```
$ git clone --branch v12.01
https://github.com/v1s1t0r1sh3r3/airgeddon.git
# already have the repo? check out this version:
$ git checkout v12.01
```

- Adds WPA3 MFP (Management Frame Protection) status analysis feature for targeted WPA3 assessments.
- Adds dynamic WPA3 plugin menu options without fixed slots, enabling flexible plugin-driven WPA3 attack workflows.
- Displays band data (2.4 GHz / 5 GHz / 6 GHz) in Evil Twin and WEP control windows, WPS attack screens, and trophy files for clearer session context.
- Improves interrupt handling so Ctrl+C or closing a worker window aborts immediately without waiting for timeouts.

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

Promptfoo ⓘ snapshot-20260715 NOTES ↗

Promptfoo is an open-source tool for testing, evaluating, and red-teaming LLM applications to detect vulnerabilities, compare outputs, and ensure AI reliability.

└──▷ TRY IT

Run a red team scan with a description and capped test cases per strategy to keep CI runtimes predictable.

```
$ promptfoo redteam generate -d 'PR #482 telecom safety check' --
numTests 10
```

Load secrets from multiple environment files (e.g., shared team vars plus local overrides) in a single eval run.

```
$ promptfoo eval --env-file .env.shared --env-file .env.local
```

Inspect recent Promptfoo service logs without leaving the terminal.

```
$ promptfoo logs
```

- New video generation providers: AWS Bedrock Nova Reel/Luma Ray 2 and Azure AI Foundry Sora.
- xAI Voice provider adds `apiBaseUrl`, `websocketUrl` override, and function call support.
- Provider config hover: view provider configuration details inline on hover in eval results.
- Test-level prompts filter and providers filter: scope prompts and providers to individual test cases.
- Support for `$VAR` syntax in file paths for environment variable interpolation.

+6 more

WAS THIS USEFUL? 👍 👎

Lakera ⓘ snapshot-20260715 NOTES ↗

Lakera Guard is an AI security platform that protects LLM-powered applications from prompt injections, jailbreaks, and other malicious inputs in real time.

Lakera adds AI Agent Security (Early Access), Policy Impact Simulator, per-detector confidence levels, and a self-harm subcategory to content moderation.

└──▷ HOW TO FIND IT

Before tightening a policy, use the Policy Impact Simulator to preview how many historical requests would have been flagged at each sensitivity level.

> 📍 In the dashboard, navigate to Policies › select a policy › Policy Impact Simulator. Adjust the sensitivity slider across L1–L4 and review the flagging-rate and category-level breakdown charts before saving.

Cover agentic pipelines by sending tool-role messages so Lakera evaluates content produced by tool calls, not just end-user turns.

```
$ curl -X POST https://api.lakera.ai/v1/guard \
  -H 'Authorization: Bearer $LAKERA_GUARD_API_KEY' \
  -H 'Content-Type: application/json' \
  -d '{"messages": [{"role": "developer", "content": "You are a
helpful assistant."}, {"role": "tool", "content": "<tool output
containing external data>"}]}'
```

- New `result` field in Guard API breakdown responses exposes per-detector confidence levels (`l1_confident` through `l5_unlikely`), matching the granularity already available in `/guard/results` .
- New `self-harm` sub-category added to the content moderator detector.
- New product: AI Agent Security (Early Access) — discovers and inventories agents, their tools, and connected MCP servers across Amazon Bedrock, Amazon Bedrock AgentCore, Google Cloud, Microsoft Copilot Studio, Salesforce Agentforce, n8n, and Relevance AI.
- AI Agent Security provides per-agent risk ratings (Critical / High / Medium / Low) with contributing factors, plus a risk-types view mapped to OWASP and MITRE ATLAS.
- New Policy Impact Simulator on the dashboard shows how different sensitivity levels and guardrail configurations would have affected historical traffic, with flagging-rate comparisons across L1–L4 and category-level breakdowns.

+8 more

WAS THIS USEFUL? 👍 👎

Veracode ⓘ Platform updates (2026-07-13) BLOG ↗

Veracode is a cloud-based application security platform that scans code for vulnerabilities, helping developers identify and fix security flaws across the software development lifecycle.

Veracode adds OAuth 2.0 credentials UI, new Reporting API filters, CMEK encryption, and Firewall Analytics in this release cycle.

└──▷ HOW TO FIND IT

Create and manage OAuth 2.0 Client credentials for automated integrations without using API key pairs.

> 📍 In the Veracode Platform, go to your account menu › API Credentials, then select 'Create OAuth 2.0 Client Credentials' and copy the generated client ID and secret for use in your integration.

- Adds `custom_severity` filter to the Reporting API Findings report for targeted severity-based querying.
- Adds six new built-in security policies to the Veracode Platform.
- Policy Settings page now supports light and dark mode.
- Reporting REST API now available in the European Region (Early Access).

└──▷ BREAKING ON UPGRADE

- ! The `/healthcheck/status` endpoint has been removed and now returns a 404 error; use the `v2/principal` endpoint in the Identity REST API instead.
- ! Success events have been removed from the Firewall dataset in Veracode Analytics.

WAS THIS USEFUL? 👍 👎

Snyk Open Source ⓘ changelog · Jun 28, 2026 BLOG ↗

Snyk Open Source is a developer security tool that automatically finds, prioritizes, and fixes vulnerabilities in open source dependencies within your projects.

Snyk Open Source adds uv SCM integration for Python and GA support for Go private dependency scanning.

└──▷ HOW TO FIND IT

Enable uv SCM support so Python teams can import uv projects and trigger PR Checks without needing the CLI.

> 📍 In the Snyk console, go to Settings › Snyk Preview for your Group or Organization and enable the uv SCM integration feature.

- Supports uv package manager in SCM integrations, enabling import of uv projects and workspaces, PR Checks, and monitoring directly from connected Git repositories — no CLI required.
- Enables Go scanning for private dependencies via private module proxies (Artifactory, Nexus) and private repositories via Broker, now generally available across all SCM integrations.

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

Cloudflare ⓘ

A broken DNSSEC rollover took down .AL. Now 1.1.1.1 tells you when validation is bypassed (2026-07-14)

5 RELEASES · 2026-07-13 → 2026-07-14 BLOG ↗ LATEST STABLE

Cloudflare is a cloud platform that provides website security, performance optimization, and DDoS protection by routing traffic through its global network.

1.1.1.1 now emits EDE 33 (Negative Trust Anchor) on responses served under an NTA, making DNSSEC bypass visible to clients.

└──▷ TRY IT

Detect whether a response from 1.1.1.1 was served under a Negative Trust Anchor — useful in monitoring scripts or incident triage when a TLD-level DNSSEC rollover is suspected.

```
$ kdig @1.1.1.1 google.al
```

- Adds EDE code 33 (Negative Trust Anchor) to all responses served while an NTA is active, signalling that DNSSEC validation was bypassed rather than silently returning an unverified answer.
- Surfaces EDE 9 (DNSKEY Missing) alongside EDE 33 during NTA incidents, giving operators and monitoring tools full visibility into both the underlying DNSSEC failure and the resolver's mitigation.

▾ 4 more releases in this issue · 2026-07-13 → 2026-07-14

WAF - WAF Release - 2026-07-14 (2026-07-14) BLOG ↗ STABLE

Cloudflare WAF adds new managed rules blocking critical RCE and memory disclosure CVEs in Citrix NetScaler and Progress Kemp LoadMaster.

- New managed rule blocks unauthenticated memory disclosure (CVE-2026-8451) targeting Citrix NetScaler ADC and Gateway appliances configured as SAML IdPs.
- New managed rule blocks unauthenticated remote code execution (CVE-2026-8037) via OS command injection in Progress Kemp LoadMaster load balancers.

WAF - WAF Release - Scheduled changes for 2026-07-20 (2026-07-14) BLOG ↗ STABLE

Cloudflare WAF adds 8 new detections covering SSRF, LFI, Adobe ColdFusion CVEs, and JS bracket-concat XSS obfuscation.

- New detection: SSRF - Restricted Protocol (rule 7fbdc9407bdb4a4eae2b3d91215e7d31), deploying in Log mode on 2026-07-20.
- New detection: SSRF - Obfuscated Host (rule 6ca512d240d848d6a0c7ef42a935ee5d), deploying in Log mode on 2026-07-20.
- New detection: LFI - Path Traversal (rule a3fb0870c38440d8a9a0eba81b0230ac), deploying in Log mode on 2026-07-20.
- New detection: Adobe ColdFusion File Upload Path Traversal (CVE-2026-48276, rule 452a04be3f73458c863d8dae61349c8b), deploying in Log mode on 2026-07-20.
- New detection: Adobe ColdFusion Path Traversal (CVE-2026-48282, rule a53a3fb491c64d74908081ee9cb61eac), deploying in Log mode on 2026-07-20.

+1 more

`Introducing Precursor: detecting agentic behavior with continuous client-side signals (2026-07-13)`

BLOG ↗ STABLE

Cloudflare launches Precursor: continuous client-side behavioral signals that extend bot detection across entire user sessions.

.

└──▷ **HOW TO FIND IT**

Enable Precursor on a zone to start collecting continuous session-level behavioral signals and feeding them into your existing bot defenses.

> 📍 In the Cloudflare dashboard, go to your zone › Security › Bots, find the Precursor section, toggle Precursor on, and select a verification mode (low-friction background observation or enforced Challenge for unverified sessions).

After enabling Precursor, investigate sessions showing signs of sustained automation — especially behavior occurring between individual requests.

> 📍 In the Cloudflare dashboard, go to Security › Security Analytics, then switch to the session-based view to filter bot management traffic by session-level signals and identify divergent visitor journeys.

- Introduces Precursor, a session-based client-side verification system that dynamically injects JavaScript into HTML responses to continuously collect behavioral signals (pointer movement, keyboard timing/rhythm, focus changes, visibility) across the full user journey — no application changes required.
- Adds session-scoped behavioral evaluation that accumulates signal throughout a session, preventing bots from resetting their behavioral signature via page refresh or new challenge.
- Detects automation patterns (linear mouse interpolation, inhuman click precision, missing physiological tremor, atypical timing) by cross-referencing multiple interaction streams in an edge-side evaluation layer with a roster of modular evaluators.
- Feeds session-level behavioral signals directly into existing bot score, challenge decisions, and security rules — improving detection precision without adding friction for legitimate users.
- Introduces session-based views in Security Analytics, enabling practitioners to analyze full visitor journeys, identify where sessions diverge from expected human behavior, and surface sessions showing sustained signs of automation.

+1 more

Challenges - Precursor introduces session-based bot detection (2026-07-13)

BLOG ↗ STABLE

Cloudflare Precursor adds session-based JavaScript bot detection with continuous behavioral re-evaluation across user sessions.

.

└──▷ **HOW TO FIND IT**

Enable Precursor from the Cloudflare dashboard to activate session-based bot detection for your zone.

> 📍 In the Cloudflare dashboard, go to Security › Bots and enable Precursor, then select your preferred mode to balance security and user experience.

- New Precursor client-side JavaScript engine continuously evaluates behavioral signals across a session for bot detection.
- Enables re-validation of challenge clearance as session behavior changes, updating bot scores with session context.
- Provides client-side visibility into bot signals where no previous detection existed.
- Integrates with existing Security Rules and supports configurable modes to balance security and user experience.

› Precursor can be enabled directly from the Cloudflare dashboard.

WAS THIS USEFUL? 👍 👎

Invicti ⓘ Release 20260709 (2026-07-09) BLOG ↗

Invicti is an automated web application security scanner that identifies vulnerabilities like SQL injection and XSS to help organizations secure their web assets.

Invicti adds LDAP sync, HashiCorp Vault integration, a new API scan profile, custom scan speed, and expanded API discovery.

└──▷ **HOW TO FIND IT**

Tune scan throughput for a sensitive target without triggering rate-limiting or WAF blocks.

📍 In the scan configuration, open Scan Speed and select Custom, then set the number of concurrent requests and the request send frequency to values appropriate for your target environment.

- › New LDAP user synchronization: automates user provisioning from OpenLDAP or Microsoft Active Directory into Invicti Platform.
- › New HashiCorp Vault integration: Secrets Manager can now retrieve credentials directly from HashiCorp Vault for scan authentication.
- › New dedicated API scan profile applied by default to all new API targets for comprehensive API vulnerability coverage.
- › New Custom scan speed option lets you set the number of concurrent requests and send frequency for precise scan throughput control.
- › Sensorless API Discovery now reports APIs found on out-of-scope sites, expanding visibility of your full API surface.

+5 more

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Sublime Security ⓘ

Platform v1.85.38 (CrowdStrike Falcon Sandbox Integration) (2026-07-13) BLOG ↗

Sublime Security is an email security platform that detects and blocks phishing, malware, and other email-based threats using customizable, rules-driven detection logic.

Sublime Security adds CrowdStrike Falcon Sandbox detonation for suspicious emails directly from the message detail view.

.

└──▷ HOW TO FIND IT

Connect your existing CrowdStrike Falcon Sandbox subscription so analysts can detonate suspicious emails without leaving Sublime.

> 📍 In the Sublime console, go to Account → Sandbox Integrations and enter your CrowdStrike Falcon Sandbox API key to enable the integration.

Detonate a suspicious message and review the full Falcon verdict without downloading or manually handling the email file.

> 📍 Open the suspicious message in the Message Detail View, click 'Send to CrowdStrike Sandbox', then view the verdict and behavioral report in the Sandbox Analysis section once detonation completes.

- Adds one-click email detonation via CrowdStrike Falcon Sandbox from the message detail view — no manual file handling required.
- New in-platform Sandbox Analysis section displays verdict (Malicious / Suspicious / Benign) and detonation environment, updating live without a page refresh.
- One-click pivot opens the full Falcon detonation report — including behavioral indicators, network activity, dropped files, and IOCs — in a new tab.
- Smart deduplication returns existing Falcon analysis results instantly for previously seen samples, preserving sandbox quota.
- Supports bring-your-own CrowdStrike Falcon Sandbox subscription; admins connect it once under Account → Sandbox Integrations.

WAS THIS USEFUL? 👍 👎

◆ Cloud Security Posture

Aikido Security ⓘ

#51 - Repository Code Quality scans, Ignore Approval Inbox and Noise Reduction for Secrets & CVE's

NOTES ↗

Aikido Security is an all-in-one developer-focused security platform that scans code, dependencies, containers, and cloud infrastructure for vulnerabilities and misconfigurations.

Aikido #51 adds repository-wide code quality scans, an ignore approval inbox, AI-powered noise reduction for secrets & CVEs, and a wave of new integrations and APIs.

└──▷ HOW TO FIND IT

Trigger a full repository code quality scan to find hotspots across the entire codebase, not just open PRs.

> 📍 In the Aikido console, go to Code Quality › Repository Scan (early access) and initiate a full codebase scan to view quality trends and refactoring hotspots.

Review and approve or reject team ignore requests before they take effect, maintaining admin control over noise suppression.

> 📍 In the Aikido console, go to the Approval Inbox and review pending ignore requests submitted by team members before approving or rejecting each.

- › New Code Quality Repository Scan (early access): scan entire codebases for quality issues, monitor trends, and identify refactoring hotspots — not just PR-level checks.
- › New Approval Inbox for Ignores: routes every ignore request through a central inbox requiring admin sign-off before issues leave the feed.
- › New AI-powered Noise Reduction for Secrets & CVEs: analyzes each secret and CVE against actual code to surface only truly exploitable findings and suppress irrelevant ones.
- › New Dashboard available to all users.
- › Adds Azure DevOps Self-Managed Server support for source code scanning.

+14 more

WAS THIS USEFUL? 👍 👎

Wiz ⓘ changelog · Jul 14, 2026 BLOG ↗

Wiz is a cloud security platform that scans and protects cloud environments by identifying vulnerabilities, misconfigurations, and risks across an organization's entire cloud infrastructure.

Wiz adds detection and IOCs for the @asyncapi npm supply chain compromise (M-RED-TEAM v6.4 malware).

- Adds detection for five malicious @asyncapi npm package versions (@asyncapi/generator 3.3.1, @asyncapi/generator-helpers 1.1.1, @asyncapi/generator-components 0.7.1, @asyncapi/specs 6.11.2 and 6.11.2-alpha.1) tied to the July 14, 2026 supply chain attack.
- Surfaces IaC coverage as a three-stage funnel metric (IaC-supportable → Tracked by IaC → Mapped to a declaration in code) within the Wiz platform to quantify how much cloud infrastructure is governed, traceable, and remediable via pull request.

WAS THIS USEFUL? 👍 👎

Sysdig Secure ⓘ Secure SaaS - July 14, 2026 BLOG ↗

Sysdig Secure is a cloud-native security platform that detects threats, enforces compliance, and protects containers, Kubernetes, and cloud infrastructure at runtime.

Sysdig Secure adds column customization for Vulnerability Management Findings reports.

└──▷ **HOW TO FIND IT**

Tailor a new Vulnerability Management Findings report to surface only the columns your team cares about, in the order that fits your workflow.

> 📍 In the console, go to Vulnerabilities › Reporting, create a new report, and use the Column Customization option to select and reorder the columns to include.

- Enables selection and reordering of columns in newly created Vulnerability Management Findings reports.

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

cilium-cli ⓘ v0.19.6 NOTES ↗

CLI to install, manage & troubleshoot Kubernetes clusters running Cilium

cilium-cli v0.19.6 adds table-json BGP output, hybrid routing mode support, Gateway API listenersets in sysdump, and TCPRoute/UDPRoute v1.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.19.6 https://github.com/cilium/cilium-cli.git
# already have the repo? check out this version:
$ git checkout v0.19.6
```

- Adds `table-json` output format to `cilium-dbg bgp peers` and `cilium-dbg bgp routes` for machine-readable BGP state.
- Includes Gateway API listenersets in `cilium sysdump` captures.
- Supports `hybrid` routing mode (`routing-mode: hybrid`), dynamically choosing native routing for same-subnet traffic and tunnel encapsulation for cross-subnet traffic.
- Upgrades TCPRoute and UDPRoute Gateway API resources to v1.
- Bumps minimum supported Cilium version to v1.16.

└──▷ BREAKING ON UPGRADE

! The minimum compatible Cilium version is now v1.16; clusters running Cilium v1.15 or older are no longer supported by this CLI version.

WAS THIS USEFUL? 👍 👎

◆ Runtime Security

NoLabs nono ⓘ v0.68.0 NOTES ↗ CODE ↗

Sandbox any AI agent in seconds - zero setup, zero latency.

nono v0.68.0 adds process-count caps, port ranges, per-OS profile overrides, domain blocking, plain HTTP proxy support, and bun/mise policy presets.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.68.0 https://github.com/nolabs-ai/nono.git
# already have the repo? check out this version:
$ git checkout v0.68.0
```

└──▷ USE IT

Block a known data-exfiltration domain at the proxy layer for all traffic through a sandboxed agent.

```json
{
  "deny_domain": ["exfil.example.com"]
}
```

Apply different filesystem grants on macOS vs Linux within a single shared profile using `platform_overrides`.

```json
{
  "platform_overrides": {
    "macos": {
      "fs_read": ["/opt/homebrew"]
    },
    "linux": {
      "fs_read": ["/usr/local"]
    }
  }
}
```

› Adds `--max-processes` flag to cap the number of processes a sandbox may spawn (enforced via cgroup v2 `pids.max`).

› Adds port range support to sandbox profiles, enabling network rules that span a

range of ports rather than individual ports.

- Adds `platform_overrides` field to profiles for per-OS patch sets, letting a single profile express different rules on macOS vs Linux.
- Adds `deny_domain` proxy configuration to explicitly block specific domains through the proxy.
- Adds `exec_paths` per-command tool-sandbox setting to support multi-call binaries (e.g. busybox-style) that need access to multiple executable paths.

+3 more

WAS THIS USEFUL? 👍 👎

NVIDIA OpenShell ⓘ v0.0.82 NOTES ↗

OpenShell is the safe, private runtime for autonomous AI agents.

OpenShell v0.0.82 adds Kubernetes sidecar supervisor topology and PVC subPath driver config support.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v0.0.82 https://github.com/NVIDIA/OpenShell.git
# already have the repo? check out this version:
$ git checkout v0.0.82
```

- Adds sidecar supervisor topology for Kubernetes deployments, enabling a new deployment model for supervisor processes.
- Supports PVC subPath in driver configuration for Kubernetes, allowing more granular persistent volume claim targeting.

WAS THIS USEFUL? 👍 👎

◆ CNAPP

Wiz Cloud ⓘ changelog · Jul 13, 2026 BLOG ↗

Wiz Cloud is a cloud security platform that identifies risks, misconfigurations, vulnerabilities, and threats across multi-cloud environments through agentless scanning.

Wiz IaC Inventory reaches GA, linking every IaC module to its live cloud deployments and managed resources.

└──▷ HOW TO FIND IT

Navigate to the IaC Inventory in the Wiz console to trace a live cloud resource back to the IaC module that provisioned it.

> 📍 In the Wiz console, go to Code › IaC Inventory, select a module to view its linked deployments and the live cloud resources it manages.

- IaC Inventory is now Generally Available, connecting every IaC module to the deployments it created and the live cloud resources it manages.
- Reconciles Wiz Code IaC scan results with Wiz Cloud runtime visibility, bridging infrastructure-as-code definitions to what is actually running.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Endpoint Security (EDR/XDR)

Huntress ⓘ

See the details of every Huntress investigation with the new Partner Investigations View (Early Access)

NOTES ↗

Huntress is a managed security platform that detects, investigates, and remediates cyber threats for small and mid-sized businesses through 24/7 expert-backed monitoring.

New Partner Investigations View (Early Access) exposes full Huntress SOC activity — including Closed-Benign outcomes — across EDR, ITDR, and SIEM.

└──▷ HOW TO FIND IT

Opt in to the new Investigations View to review all SOC investigations — including benign closures — from the past 90 days.

📍 In the Huntress portal, go to the top nav and select "Investigations", then click the "Try the new investigations view" banner to opt in.

› Adds Partner Investigations View (Early Access) showing all completed SOC investigations — both Reported and Closed-Benign — across Managed EDR, ITDR, and SIEM, not just those that became incident reports.

› Each investigation includes a chronological timeline of signals reviewed, actions taken, remediations applied, and final outcome.

› Automatically surfaces completed investigations from the last 90 days upon opt-in.

WAS THIS USEFUL? 👍 👎

Trend Vision One ⓘ

Credit transaction records now available (2026-07-06) BLOG ↗

Trend Vision One is a unified cybersecurity platform that provides extended detection and response (XDR) across endpoints, networks, email, and cloud environments.

Trend Vision One adds a self-service Credit Transaction view with balance history, drawdown details, and downloadable usage reports.

└──▷ HOW TO FIND IT

Review which solution packages drove credit consumption last month and download a full-month report for record-keeping.

> 📍 In the console, go to TrendAI Flex Licensing → Platform Usage and Credits › Credit transaction view, set the time period filter to 'Last month', expand the relevant drawdown entry to see the per-package breakdown, then select the package and click Download to export the full-month spreadsheet bundle.

- New Credit transaction view in Platform Usage and Credits provides a chronological ledger of every credit-affecting event: purchases, monthly drawdowns, expirations, adjustments, license transfers, and licensing-model transitions.
- Balance history ledger shows transaction date, event type, credit amount, and running balance, filterable by time period (current month, last 3/6/12 months, or custom date range) and by transaction type.
- Drawdown entries expand to reveal per-package credit breakdowns with direct navigation into detailed monthly views.
- Monthly drawdown view distinguishes live in-progress estimates for the current month from finalized past-month usage, with day-by-day breakdowns per solution package.
- Supports downloading individual day usage reports for the current month or full-month spreadsheet bundles covering all packages.

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines ⓘ Reuse recent App endpoint responses (2026-07-14)

2 RELEASES · 2026-07-14 | BLOG ↗ | LATEST | STABLE

Tines is a no-code automation platform that helps security and operations teams build workflows to automate repetitive tasks and orchestrate tools.

Tines App endpoints can now cache and reuse recent responses for identical requests, cutting latency and redundant story runs.

› Enables response reuse on App endpoints so identical incoming requests return a cached result without re-executing the story.

▾ 1 more release in this issue · 2026-07-14

Find and replace in stories (2026-07-14) BLOG ↗ STABLE

Tines adds find-and-replace across entire stories for faster bulk edits.

└──▷ HOW TO FIND IT

Bulk-update a hostname, credential name, or URL that appears across many actions in a story without editing each one individually.

> 📍 In the story editor, open Find and Replace, enter the text to find and the replacement text, then apply to update all matching instances across the story.

› Adds find-and-replace functionality to search and update text throughout an entire story at once.

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Splunk Security Content ⓘ v6.2.0 NOTES ↗

Splunk Security Content

Splunk Security Content v6.2.0 adds 10 new detections spanning Linux Dirty Frag, Phantom Stealer, AWS Bedrock Claude AI abuse, and browser process injection.

└──▷ GET THIS VERSION

```
$ git clone --branch v6.2.0
https://github.com/splunk/security_content.git
# already have the repo? check out this version:
$ git checkout v6.2.0
```

- New detection: Linux Dirty Frag Kernel Privilege Escalation (CVE-2026-43284 & CVE-2026-43500) — identifies high-frequency splice() syscall activity followed by setuid binary execution within the same audit session.
- New analytic story: Phantom Stealer — expands Windows infostealer coverage with a new detection for unauthorized WinSCP security configuration folder access, plus enhanced tagging of existing analytics for credential theft, PowerShell abuse, process injection, and data exfiltration.
- New detection: Windows Uncommon Remote Thread Creation In Browser Process — strengthens visibility into CreateRemoteThread-based process injection targeting browser processes using native Sysmon Event ID 8 field mappings.
- New analytic story: Suspicious AWS Bedrock Claude Activities — introduces 7 new detections covering cross-region inference abuse, excessive token consumption, high-risk filesystem/exec tool invocation, hostile prompt sentiment, prompt injection, sensitive data in prompts, and unusually large prompt submissions.
- Updated PowerShell ScriptBlock analytics to omit oversized ScriptBlockText fields from finding messages and convert detections to Anomaly type for clearer triage.

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

MISP ⓘ v2.5.43 NOTES ↗

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

MISP 2.5.43 adds collection sync between instances, environment-variable settings, Pivotick pivot explorer, and TAXII Bearer auth.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.5.43 https://github.com/MISP/MISP.git
# already have the repo? check out this version:
$ git checkout v2.5.43
```

└──▷ HOW TO FIND IT

Enable collection push to a remote peer so newly created collections are automatically synchronised to that instance.

> 📍 In the MISP UI, go to Sync Actions › List Servers, edit the target server, and enable the push_collections and pull_collections toggles under the synchronisation options.

- Adds collection synchronisation between MISP instances in both pull and push directions, with per-server `pull_collections` / `push_collections` toggles, feature negotiation with pagination, and a `collections.locked` origin-protection flag.
- Supports environment variables as a third settings source alongside config file and database, enabling cleaner containerised and IaC deployments.
- Introduces Pivotick as an initial drop-in replacement for the legacy event graph, including a draft drag-and-drop reference editor.
- Adds Bearer authentication for TAXII servers and a streamlined add flow for basic auth; the TAXII 'API key' field is renamed to Token and obfuscated in the server view.
- Extends the Overmind (Bootstrap 5) UI to user index, categories & types, application/audit/access logs, galaxies/galaxy clusters/galaxy relationships, and proposals screens, plus inline tag/galaxy addition from event view.

+2 more

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Vulnerability Management

Edgescan ⓘ Release Notes - 2nd July 2026 NOTES ↗

Edgescan is a cloud-based vulnerability management platform that continuously discovers, assesses, and prioritizes security vulnerabilities across an organization's entire digital attack surface.

Edgescan adds custom policy compliance insights, split retest permissions, self-service domain management, and a Credential Vault across this release.

- New Custom Policy Compliance insight: upload company policy documents and see how vulnerabilities align with those policies.
- New `manage-retests` permission lets admins delegate retest execution without granting access to start new assessments.
- Self-service creation, renaming, and removal of internal domain suffixes directly on the Organizations Scanning tab.
- Hostname validation on asset location entry prompts for a fully qualified domain name when a bare machine name is entered.
- Super-user email alert when a new user is created via SSO, enabling prompt permission review.

+11 more

└──▷ **BREAKING ON UPGRADE**

! The Shared Credentials feature is renamed to Credential Vault across the application and API; any integrations, scripts, or documentation referencing the old name will need to be updated.

WAS THIS USEFUL? 👍 👎

defectdojo ⓘ 3.1.100 NOTES ↗

Open-Source Unified Vulnerability Management, DevSecOps & ASPM

DefectDojo 3.1.100 adds FTS+trigram global search indexes, Jira close/reopen transition fields, and exposes dedupe policy on the Test API.

└──▷ **GET THIS VERSION**

```
$ git clone --branch 3.1.100 https://github.com/DefectDojo/django-DefectDojo.git
# already have the repo? check out this version:
$ git checkout 3.1.100
```

- Adds full-text search (FTS) and trigram GIN indexes for global search, requiring a settings and database migration update.
- Supports custom fields on Jira close/reopen transitions via a new database migration.
- Exposes the effective dedupe matching policy on the Test API endpoint.

└──▷ **BREAKING ON UPGRADE**

! The FTS + trigram GIN indexes for global search require changes to `settings.dist.py` / `local_settings.py` and a database migration — existing deployments must apply both before upgrading.

WAS THIS USEFUL? 👍 👎

Rapid7 InsightVM

changelog · Jul 13, 2026

BLOG ↗

Rapid7 InsightVM is a vulnerability management platform that continuously scans networks to identify, prioritize, and help remediate security risks across an organization's infrastructure.

InsightVM 8.52.0 adds fingerprinting for AI tools, Microsoft Intune-managed apps, and Splunk Enterprise.

- New fingerprinting coverage for AI tools enables detection and inventory of AI software on scanned assets.
- New fingerprinting support for Microsoft Intune-managed applications expands visibility into managed endpoint software.
- New fingerprinting capability for Splunk Enterprise improves detection of Splunk deployments during scans.

WAS THIS USEFUL?

◆ Attack Surface & Exposure Management

Qualys CyberSecurity Asset Management ⓘ

changelog · Jul 14, 2026 BLOG ↗

Qualys CyberSecurity Asset Management continuously discovers, inventories, and assesses all IT assets across hybrid environments to eliminate security blind spots and reduce cyber risk.

Qualys ETM Identity unifies identity risk, attack path analysis, and automated remediation into CSAM's risk model.

- New Qualys ETM Identity module discovers risky identities and correlates identity and asset risk into a unified risk model.
- Supports attack path analysis and domain trust mapping to visualize lateral movement exposure across Active Directory environments.
- Introduces Identity TruRisk scoring to quantify identity risk based on criticality and associated misconfiguration severity.
- Detects Pass-the-Hash (PtH) risk conditions including legacy NTLM authentication, cached credentials, weak authentication settings, and excessive admin privileges.
- Maps DCSync exposure in identity graphs, surfacing identities with replication rights before they can be exploited.

+2 more

WAS THIS USEFUL? 👍 👎

runZero ⓘ runZero 5.0.260714.0 (2026-07-14) BLOG ↗

runZero is a network discovery and asset inventory platform that scans environments to identify and catalog all connected devices, systems, and services.

runZero 5.0.260714.0 adds crown jewel status and Purdue level to the Dragos integration.

- Adds crown jewel status and Purdue level fields to assets surfaced via the Dragos integration.
- Vulnerability groups inventory now displays a meaningful error message when a search contains unsupported terms.

WAS THIS USEFUL? 👍 👎

Censys ⓘ July 13, 2026 (2026-07-13) BLOG ↗

Censys is an internet intelligence platform that continuously scans and indexes internet-facing assets, helping security teams discover and monitor exposed infrastructure and vulnerabilities.

Censys Assistant gains page-aware context and 8 new fingerprints added to the Platform.

└──▷ HOW TO FIND IT

Investigate an unfamiliar service on a host without copy-pasting asset details — open the Assistant directly from a host page and ask about exposed services in context.

> 📍 In the Platform, navigate to a host detail page, open the Censys Assistant panel, and ask 'What services on this host are unusual or potentially exposed?' — the Assistant automatically uses the current host as context.

- Censys Assistant now automatically reads the current page (host, certificate, web property, search result, or collection) as context when opened, enabling deeper questions about specific assets without manually specifying them.
- Adds 8 new fingerprints to the Platform: Chatto, RedHat Cockpit, D-Link DAP Series Access Point, BigBlueButton, Monospace Directus, Google Mod PageSpeed, Hugo, and Streamlit.

WAS THIS USEFUL? 👍 👎

Tenable One

changelog · Jul 13, 2026

BLOG ↗

Tenable One is an exposure management platform that provides unified visibility across attack surfaces to help organizations identify, prioritize, and remediate cybersecurity risks.

Tenable One Cloud Exposure earns FedRAMP High and IL5 authorization, enabling use in highly sensitive federal and intelligence environments.

- Achieves FedRAMP High authorization, expanding support beyond the existing FedRAMP Moderate status to highly sensitive federal environments.
- Achieves IL5 authorization, enabling use by intelligence agencies and mission-critical use cases that previously required separate tooling.
- Delivers unified CNAPP capabilities within strictly regulated federal cloud ecosystems with strict data isolation requirements.

WAS THIS USEFUL?

IDENTITY, ACCESS & DATA PROTECTION

◆ Data Security & DLP

Immuta ⓘ snapshot-20260715 NOTES ↗

Immuta is a data security platform that automates access control, privacy protection, and policy enforcement across cloud data environments.

- Adds automated sensitive data discovery for the Amazon Redshift viewless integration, supporting regex, dictionary, and column name regex identifier types with automatic tag application.
- Adds Slack and Microsoft Teams event-driven notifications for the Request app (approvals, access changes, requests), now generally available.
- Expands Teradata integration masking support to include constant and hash masking in addition to existing null masking.
- Revokes data owner grants when a data source is disabled (behavior change rolling out via opt-in period starting June 30).
- Review Assist now incorporates request form responses as additional context in its AI-powered access request recommendations.

└──▷ **BREAKING ON UPGRADE**

- ! When a data source is disabled in Immuta, Immuta now revokes data owners' Immuta-managed grants in the data platform — previously, disabling a data source did not remove those grants. This change follows the behavior change release process (on by default: 8/1; enabled for all: 9/1).
- ! Starburst (Trino) principal name matching is now case-insensitive; previously, Trino principals had to match the exact capitalization of the corresponding user or service account in Immuta. This is on by default starting 7/1 and enabled for all accounts on 8/1.

WAS THIS USEFUL? 👍 👎

Ubiq Security ⓘ snapshot-20260715 NOTES ↗

Ubiq Security is a developer platform providing APIs and SDKs that enable applications to encrypt and decrypt sensitive data using structured, format-preserving encryption.

Ubiq overhauls dataset access controls with Access Groups and tagging, adds advanced structured encryption config, and expands library support.

└─▷ HOW TO FIND IT

Enable automatic IDP role-based dataset access by creating an Access Group whose name matches an IDP role — members gain dataset access without manual assignment.

> 📍 In the Ubiq Dashboard, go to Identities › Access Groups › Create Access Group, name the group to match your IDP role, assign the target Datasets, and save. IDP users with that role will be granted access automatically.

Pre-warm the key cache on startup to eliminate first-use latency in latency-sensitive Java services before any encrypt/decrypt calls.

```java
ubiqSession.loadCache();
```

- Introduces Access Groups to replace the Dataset Group → Identity model, granting dataset access to API Keys or IDP users independently of dataset organization.
- Advanced Dataset Configuration for Structured Encryption now lets operators define encryption behavior for dates, numerics, short fields, and large character sets at the dataset policy level — no custom code required.
- Unified Identities section consolidates API Keys and IDP-managed users, with a new per-identity access graph for at-a-glance visibility into access groups and datasets.
- Platform resiliency upgrade enables zero-downtime deployment of core system changes to APIs and encryption services.

WAS THIS USEFUL? 👍 👎

DigiCert CertCentral ⓘ July 14, 2026 NOTES ↗

DigiCert CertCentral is a certificate management platform that allows organizations to issue, manage, renew, and automate SSL/TLS and other digital certificates.

CertCentral adds Persistent DNS TXT Record DCV, enabling one-time DNS setup for repeated domain revalidations.

└──▷ HOW TO FIND IT

Enable the Persistent DNS TXT Record DCV method for your account so it appears in all DCV method menus.

> 📍 In the CertCentral menu, go to Settings › Preferences. Expand Advanced Settings. Under Domain Control Validation (DCV) › DCV methods, select Persistent DNS TXT Record. Click Save Settings.

- Adds Persistent DNS TXT Record as a new domain control validation (DCV) method, allowing a single DNS TXT record to satisfy repeated revalidations without creating new records each cycle.
- Supports an Account URI option — one shared persistent URI to validate any domain across the entire CertCentral account, simplifying multi-domain DNS management.
- Supports a Unique URI option — a domain-specific persistent URI to avoid publicly linking domains through shared DNS records.
- Enables Persistent DNS TXT Record DCV on certificate request forms, the Domains page (add/validate/revalidate), and pending OV, EV, and DV TLS certificate orders once activated in account preferences.

WAS THIS USEFUL? 👍 👎

Cyera ⓘ Access Trail for Google Workspace 5 RELEASES · seen 2026-07-15

NOTES ↗ LATEST STABLE

Cyera is a cloud data security platform that discovers, classifies, and protects sensitive data across cloud environments to reduce risk and ensure compliance.

Cyera expands Access Trail to Google Workspace with audit visibility, event enrichment, saved filters, and access revocation.

- Adds Access Trail coverage for Google Workspace, including My Drive and Shared Drives audit visibility.
- Enriches access events with data classification and identity context for deeper investigation.
- Introduces saved high-risk filters to quickly surface and revisit critical access patterns.
- Enables optional access revocation directly from Access Trail findings in Google Workspace.

▾ **4 more releases in this issue** · seen 2026-07-15

Browser Shield Policy Creation NOTES ↗ STABLE

Cyera Browser Shield adds policy creation and a template catalog to enforce data controls on browser-based AI workflows.

└──▷ **HOW TO FIND IT**

When a new shadow AI destination is flagged in alerts, use the Browser Shield policy editor to select a provider, apply a template, configure rules, and deploy — without building from scratch.

> 📍 In the Cyera console, go to Browser Shield › Policies, select "Create Policy", choose a provider, pick a template from the Policy Catalog, configure your data classification rules, and click Deploy.

- New Policy Creation editor for Browser Shield lets security teams configure and deploy data-leak policies for browser-based AI tools in a single workflow.
- New Policy Catalog provides pre-built templates so teams can start from a baseline rather than a blank editor for each new AI surface.
- Policies distinguish managed AI tools from shadow AI destinations, enabling enforcement aligned to how employees actually use AI.

Latest Integrations - June NOTES ↗ STABLE

Cyera adds eight new ecosystem integrations and extends Claude Enterprise support in its June release.

- Extends Claude Enterprise integration for AI-driven data security workflows.
- Adds integration with Abnormal Security for email and collaboration threat response.
- Adds integration with Cohesity for data protection and backup coverage.
- Adds integration with Cato Networks for network security enforcement.
- Adds integration with Island Enterprise Browser for browser-level data policy enforcement.

+5 more

Omni DLP Memories NOTES ↗ STABLE

Cyera Omni DLP Memories retains investigation context across alerts so analysts build on prior decisions instead of starting from scratch.

.

- Adds persistent investigation context across DLP alerts, retaining history for users, destinations, organizations, and departments to eliminate repeated triage of recurring patterns.
- New dedicated Memories view lets analysts review and delete stored entries to keep automation predictable and auditable.

Remediation Center NOTES ↗ STABLE

Cyera launches Remediation Center: a dedicated workspace for data owners to triage and resolve assigned data exposures.

.

└──▷ **HOW TO FIND IT**

Route a data exposure issue to a data owner so they can act on it directly in the Remediation Center without security team involvement.

> 📍 In the Cyera console, open a finding and assign it to a data owner. The owner receives a consolidated notification and can log in via SSO or OTP to access their Remediation Center, where the issue appears in their To Do queue.

- New Remediation Center workspace gives data owners a dedicated interface to triage and resolve data security issues assigned to them.
- Adds a To Do vs. Completed workflow so remediation progress is clearly tracked and measurable.

- Consolidated notifications keep data owners informed of new assignments without manual coordination from security teams.
- Event logs provide an audit trail of remediation activity, including what was closed and when.
- Supports secure data owner access via SSO or OTP, enabling participation without requiring full platform credentials.

WAS THIS USEFUL? 👍 👎

Varonis ⓘ Secure Claude Code and Claude Cowork with Varonis Atlas

NOTES ↗

Varonis is a data security platform that automatically discovers, classifies, and protects sensitive data while detecting and responding to insider threats and cyberattacks.

Varonis Atlas adds native coverage for Claude Code and Claude Cowork with runtime guardrails and AI activity monitoring.



- Adds direct integration with Claude Code and Claude Cowork, extending Atlas coverage across the full Anthropic enterprise Claude suite.
- Enables runtime guardrails that can block, modify, or alert on risky AI behavior in real time.
- New AI activity monitoring detects exposure of sensitive data, credentials, API keys, and regulated information with user, project, resource, and token-usage context.
- Provides visibility into agent artifacts — skills, memory files, and MCP configurations — to surface persistent instructions and detect manipulation attempts.
- Delivers a complete inventory of agents, tools, and supporting resources across Claude Code, Claude Cowork, Claude Enterprise, and Claude Platform.

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

SailPoint ⓘ

Enhancement: Non-Employee Risk Management Users Connector - Automatic Synchronization (2026-07-14)

BLOG ↗

SailPoint is an identity security platform that helps organizations manage and govern user access, permissions, and credentials across enterprise systems and applications.

NERM Users connector gains real-time ISC sync toggle and UI-based role assignment for non-employee accounts.

.
.
.
.

└──▷ HOW TO FIND IT

Enable real-time ISC sync so that every NERM user or role change immediately triggers an aggregation in Identity Security Cloud, eliminating propagation delay.

> 📍 In the NERM Admin UI, go to Admin › System › Identity Security Cloud Connection Settings › USERS tab, set the 'Sync with Identity Security Cloud' toggle to ON, confirm or enter the Source ID, then click Save.

Assign a role to a non-employee user directly in the UI during implementation, without needing API access.

> 📍 In the NERM Admin UI, go to Admin › Lifecycle › User Roles, select the target user, and assign or unassign the desired role.

- Adds a new 'Sync with Identity Security Cloud' toggle in Admin > System > Identity Security Cloud Connection Settings > USERS tab, triggering immediate account or entitlement aggregation on any NERM user/role change instead of waiting for periodic aggregation.
- Adds a Source ID field to the USERS tab, allowing NERM to auto-detect an existing NERM Users connector source or optionally create one automatically when the sync toggle is first enabled.
- Enables NERM admins to assign and unassign roles directly to users from Admin > Lifecycle > User Roles in the Non-Employee Risk Management Admin UI, a capability previously limited to the API.

WAS THIS USEFUL? 👍 👎

1Password ⓘ 1Password for Mac 8.12.28 (2026-07-14)

3 RELEASES · 2026-07-13 → 2026-07-14 BLOG ↗ STABLE

1Password is a password manager that securely stores, generates, and autofills passwords, passkeys, and sensitive information across devices and browsers.

1Password 8.12.28 adds exact-phrase search, Universal Autofill for HTTP auth prompts, and a unified Developer settings section.

└──▷ HOW TO FIND IT

Look up an item by exact IP address or dotted string without partial-match noise.

> 📍 In the 1Password search bar, type "10.1.2.3" (with double quotes) to retrieve items matching that exact phrase.

Access all developer integrations (CLI, SDKs, MCP) from one place instead of hunting across multiple settings screens.

> 📍 In the 1Password app, go to Settings › Developer to find 1Password CLI, SDKs, and MCP client configuration grouped together.

▾ 2 more releases in this issue · 2026-07-13 → 2026-07-14

1Password for Windows 8.12.28 (2026-07-14) BLOG ↗ STABLE

1Password for Windows adds exact-phrase search with special characters and consolidates Developer settings into one section.

└──▷ HOW TO FIND IT

Find a vault item by exact IP address or dotted string without partial-match noise.

> 📍 In the 1Password search bar, type "10.1.2.3" (with double quotes) to retrieve items matching that exact string.

Access all developer integrations (CLI, SDKs, MCP clients) from one place instead of hunting across multiple settings pages.

> 📍 In the 1Password app, go to Settings › Developer to find CLI, SDKs, and MCP client integrations consolidated in a single section.

1Password CLI 2.35.0 (2026-07-13) BLOG ↗ STABLE

› Adds Shell Plugin support for Cline CLI, CrateDB CLI, Cursor CLI, Descope CLI, Exercism CLI, Expo and EAS CLIs, GitHub Copilot CLI, Google Gemini AI API CLI,

JetBrains Junie CLI, Kiro CLI, OpenCode CLI, OpenTofu CLI, PyPI (twine, flit, hatch), and UpCloud CLI — enabling Touch ID and other unlock options for each.

› GitHub shell plugin now provisions `GH_ENTERPRISE_TOKEN` for GitHub Enterprise Server hosts and supports authenticating to both github.com and Enterprise simultaneously when separate credentials are configured.

› Redis CLI shell plugin now supports environment variable-based credential provisioning.

› Oh Dear shell plugin now checks for `~/.ohdear/config.json` and imports credentials automatically.

└─▷ **BREAKING ON UPGRADE**

! The deprecated `zsh.initExtra` option in the nix shell plugin has been replaced with `zsh.initContent`.

! The `awslogs` CLI function has been renamed to capitalize CLI for consistency.

WAS THIS USEFUL? 👍 👎

Auth0 ⓘ

Dashboard Search for Roles Now in Beta (2026-07-14) BLOG ↗

Auth0 is a cloud-based identity platform that provides authentication and authorization services, enabling developers to securely manage user logins for applications.

Auth0 Dashboard now supports real-time Role search by ID and name, available in Public Beta.

└─▷ **HOW TO FIND IT**

Quickly locate a specific Role without scrolling through paginated lists — useful when managing large numbers of roles.

📍 In the Auth0 Dashboard, go to User Management › Roles and type a Role name or ID into the search bar to filter results in real time.

› Adds real-time search for Roles by ID and name in the Auth0 Dashboard, replacing paginated list scrolling (Public Beta, rolling out to Public Cloud tenants).

WAS THIS USEFUL? 👍 👎

JumpCloud

JumpCloud Agent Release Notes for July 13, 2026 (2026-07-13) BLOG ↗

JumpCloud is a cloud-based directory platform that manages user identities, devices, and access to IT resources across organizations securely.

JumpCloud Agent 2.147.2 adds AWS Client VPN authentication and a Windows App Catalog in the system tray.

- Supports AWS Client VPN authentication, enabling managed devices to verify posture and connect to AWS VPN gateways using JumpCloud identity (macOS and Windows).
- Adds App Catalog to the Windows tray app, letting users browse, search, and manage software applications directly from the system tray.
- Requires users to supply a reason when submitting Device Admin approval requests, aligning the workflow with security best practices.

WAS THIS USEFUL? 👍 👎

Microsoft Entra ⓘ changelog · Jul 13, 2026 BLOG ↗

Microsoft Entra is a cloud-based identity and access management platform that secures user authentication, manages permissions, and controls access to applications and resources.

Microsoft Entra ID makes passkeys the default MFA method and retires native SMS/voice auth by February 2027.

└──▷ HOW TO FIND IT

Identify which users are still enabled for SMS or voice so you can prioritize them for passkey rollout before the September 1, 2026 auto-enrollment deadline.

> 📍 In the Entra admin center, go to Protection › Authentication methods › Policies, review which users or groups have SMS or Voice enabled, then navigate to Protection › Authentication methods › Registration campaign to enable passkey nudging for those users.

- Starting September 1, 2026, users enabled for SMS or voice MFA are automatically enabled for passkeys and prompted to register one during their next MFA sign-in.
- Supports synced passkeys (iCloud Keychain, Google Password Manager) and device-bound passkeys (Microsoft Authenticator, Entra passkey on Windows, FIDO2 security keys) as first-class authentication options.
- New Microsoft Security Store partner marketplace enables organizations that still require SMS or voice to select, configure, and manage third-party telecom providers starting October 30, 2026.
- Registration campaigns now available to prompt users to register a passkey at scale during MFA sign-in flows.

└──▷ BREAKING ON UPGRADE

- ! On February 1, 2027, Microsoft-provided SMS and voice authentication is retired; users relying on these methods will be required to register a passkey before they can sign in, with no opt-out option.
- ! After February 1, 2027, automatic passkey registration prompts will be enforced for all users in all tenants with no opt-out option.

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

DNSFilter ⓘ 7/14 July 14 - iOS Roaming Client v1.4.4 (2026-07-14)

2 RELEASES · 2026-07-14 | BLOG ↗ | LATEST | STABLE

DNSFilter is a cloud-based DNS security tool that blocks malicious websites, filters harmful content, and protects networks from cyber threats in real time.

iOS Roaming Client v1.4.4 adds automatic MDM site reassignment, stronger admin PIN protection, and refreshed branding.

- Supports syncing user name, hostname, and device tag changes from MDM configuration profiles to the Dashboard without requiring a Site Secret Key change.
- Enables automatic site reassignment when a Site Secret Key changes in the MDM configuration profile, allowing fleet migrations without reinstalls or policy gaps.
- Adds progressive delays between incorrect admin PIN attempts to make automated guessing impractical while keeping legitimate retries fast.
- Refreshes app icons, visuals, and UI elements to match current DNSFilter branding.
- Enables diagnostic logging by default on new installs so Support can diagnose early issues from first run.

▾ 1 more release in this issue · 2026-07-14

07/14 July 14 – Web Application and API Update (2026-07-14) | BLOG ↗ | STABLE

DNSFilter adds CyberSight Data Export for SIEM integration and clearer Mobile Roaming Client auto-registration status display.

└──▷ HOW TO FIND IT

Route CyberSight threat data into your SIEM alongside DNS logs by enabling CyberSight Data Export in the DNSFilter dashboard.

> 📍 In the console, go to Settings › Data Export and enable CyberSight Data Export to begin forwarding CyberSight data to your configured SIEM destination.

- Adds CyberSight Data Export to all Data Export customers, enabling SIEM ingestion of CyberSight data alongside existing DNS log exports.
- Automatic Registration setting now surfaces its 7-day duration and an explicit 'Ends on [date]' status for Mobile Roaming Client, replacing the previous helper text.

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Kiro ⓘ Faster Sessions, Compaction Fixes, and PowerShell Trust

2 RELEASES · seen 2026-07-15 NOTES ↗ LATEST STABLE

Kiro is an AI-powered IDE by AWS that uses "specs" to translate requirements into structured plans, hooks, and code for building production-ready software.

Kiro 1.0.138 adds full PowerShell trust support on Windows and MCP tool recovery from transient network failures.

- Adds full PowerShell trust support on Windows for Kiro sessions.
- MCP tools now recover from transient network failures instead of failing silently.

▾ 1 more release in this issue · seen 2026-07-15

OpenAI GPT-5.6 Sol, Terra, and Luna now available NOTES ↗ STABLE

OpenAI GPT-5.6 Sol, Terra, and Luna are now available in Kiro across IDE, CLI, and Web.



└──▷ HOW TO FIND IT

Use Sol for complex, multi-step spec-driven implementation or long-horizon refactors where maximum coding capability is needed.

📍 In the Kiro IDE, CLI, or Web, open the model selector and choose GPT-5.6 Sol for your agent or chat session.

Use Luna for high-frequency, low-latency tasks (e.g., autocomplete, quick edits) to minimize Kiro credit consumption at 0.6x multiplier.

📍 In the Kiro IDE, CLI, or Web, open the model selector and choose GPT-5.6 Luna for your agent or chat session.

- Adds OpenAI GPT-5.6 Sol (flagship), Terra (balanced), and Luna (fast/low-cost) model tiers to Kiro's IDE, CLI, and Web interfaces.
- Supports 272K context window across all three GPT-5.6 tiers.
- Enables longer autonomous runs with tool-coordinating mini-programs that reduce round-trips, available across all three tiers.
- Supports cross-region inference across us-east-1 and eu-central-1 for Pro, Pro+, Pro Max, and Power customers.

WAS THIS USEFUL? 👍 👎

Claude Code ⓘ v2.1.210 2 RELEASES · 2026-07-14 NOTES ↗ CODE ↗

LATEST STABLE

Claude Code is an agentic coding tool that lives in your terminal, understands your codebase, and helps you code faster by executing routine tasks, explaining complex code, and handling git workflows - all through natural language commands.

Claude Code v2.1.210 adds a live tool timer, memory overflow errors, screen-reader mode announcements, and agent input-waiting counts.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.210 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.210
```

- Adds a live elapsed-time counter to the collapsed tool summary line so long-running tool calls visibly tick instead of appearing frozen.
- Adds a startup warning when permission rules use Write(path), NotebookEdit(path), or Glob(path) — directing users to Edit(path) or Read(path) instead.
- Memory writes that would push a MEMORY.md index over its read limit now surface an explicit error instead of silently truncating content.
- Screen reader mode now announces permission mode changes aloud when cycling through modes with Shift+Tab.
- The agents footer hint now displays how many background agents are waiting on user input, with brief color emphasis when the count changes.

+3 more

▾ 1 more release in this issue · 2026-07-14

v2.1.208 NOTES ↗ CODE ↗ STABLE

Claude Code v2.1.208 adds screen reader mode, vim insert remaps, corporate process wrapper, and fullscreen mouse support.

└──▷ GET THIS VERSION

```
$ git clone --branch v2.1.208 https://github.com/anthropics/claude-code.git
# already have the repo? check out this version:
$ git checkout v2.1.208
```

└──▷ **TRY IT**

Enable screen reader-compatible plain-text output for assistive technology users in a one-off session.

```
$ claude --ax-screen-reader
```

Persist screen reader mode across all sessions via settings instead of passing the flag every time.

```json
# In your Claude Code settings (JSON)
{ "axScreenReader": true }
```

Route all Claude Code subprocess spawns through a corporate launcher in a managed enterprise environment.

```
$ export CLAUDE_CODE_PROCESS_WRAPPER=/usr/local/bin/corp-launcher claude
```

- Adds `--ax-screen-reader` flag (also `CLAUDE_AX_SCREEN_READER=1` env var or `"axScreenReader": true` in settings) for opt-in plain-text rendering compatible with screen readers.
- Adds `vimInsertModeRemaps` setting to map two-key vim insert-mode sequences (e.g. `jj` → Escape) without leaving the editor.
- Adds `CLAUDE_CODE_PROCESS_WRAPPER` env var so every Claude Code self-spawn routes through a corporate launcher executable, enabling enterprise wrapper enforcement.
- Adds mouse-click support for multi-select menus and "Other" input rows in fullscreen mode.
- Up to 7x faster tool rounds in print/SDK sessions with many MCP tools via cached tool-pool assembly.

+3 more

WAS THIS USEFUL? 👍 👎

OpenCode ⓘ v1.18.0 2 RELEASES · 2026-07-13 → 2026-07-14 NOTES ↗

CODE ↗ LATEST STABLE

The open source coding agent.

OpenCode v1.18.0 completes Desktop v2 migration with a new layout-switch setting and improved file comments in the session timeline.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.18.0 https://github.com/anomalyco/opencode.git
# already have the repo? check out this version:
$ git checkout v1.18.0
```

- Adds a setting to switch between the new Desktop v2 and old layouts during the transition period.
- Completes the Desktop v2 migration, including upgrade handling and first-launch onboarding flow.
- Improves file comments display in the Desktop session timeline.

▾ 1 more release in this issue · 2026-07-13 → 2026-07-14

v1.17.19 NOTES ↗ CODE ↗ STABLE

OpenCode v1.17.19 adds per-prompt model selection, middle-click tabs, and an interface-switching setting in the desktop app.

└──▷ GET THIS VERSION

```
$ git clone --branch v1.17.19
https://github.com/anomalyco/opencode.git
# already have the repo? check out this version:
$ git checkout v1.17.19
```

- Adds per-prompt model selection in the composer, letting you switch models on a message-by-message basis.
- Adds middle-click to open sessions in a new tab in the desktop app.
- Adds a temporary setting to toggle between the old and new interface in the desktop app.
- Redesigns attachment cards and file comment chips in the new interface.

› Updates the review panel with persistent file browsing, improved file tabs, and easier open-in-app actions.

+2 more

WAS THIS USEFUL? 👍 👎

Pi ⓘ v0.80.7 NOTES ↗

AI agent toolkit: unified LLM API, agent loop, TUI, coding agent CLI

Pi v0.80.7 adds cache-friendly dynamic tool loading, toolChoice for OpenAI/Codex Responses, Fable 5 xhigh/max thinking, and a Ctrl+X message copy shortcut.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.80.7 https://github.com/earendil-works/pi.git
# already have the repo? check out this version:
$ git checkout v0.80.7
```

› Adds cache-friendly dynamic tool loading: extensions can inject tools during execution while Anthropic and OpenAI Responses models preserve prompt-cache prefixes.

› Adds `toolChoice` support for OpenAI and Codex Responses, including required and named tool selection.

› Adds native `xhigh` and `max` thinking levels for Claude Fable 5 across all generated provider catalogs.

› Adds `Ctrl+X` shortcut to copy the last assistant message in the transcript, or the selected message in `/tree`.

└──▷ BREAKING ON UPGRADE

! The `compat.sendSessionIdHeader` flag has been removed from `models.json` for `openai-responses` models. Replace `sendSessionIdHeader: false` with `sessionAffinityFormat: "openai-nosession"` in your `models.json`; the new field also accepts `"openai"` and `"openrouter"`.

WAS THIS USEFUL? 👍 👎

Goose ⓘ v1.43.0 2 RELEASES · 2026-07-13 → 2026-07-14 NOTES ↗ CODE ↗

LATEST STABLE

an open source, extensible AI agent that goes beyond code suggestions - install, execute, edit, and test with any LLM

Goose v1.43.0 adds per-message cost/token stats, OllamaCloud provider, `--edit` session flag, TLS for ACP serve, and six new model providers.

└──▷ **GET THIS VERSION**

```
$ git clone --branch v1.43.0 https://github.com/aaif-goose/goose.git
# already have the repo? check out this version:
$ git checkout v1.43.0
```

└──▷ **TRY IT**

Review and trim a session's conversation before branching it into a new task, avoiding stale context.

```
$ goose session --edit
```

- Adds `--edit` session flag to edit conversation history before forking a session.
- New per-message usage stats UI showing tokens, cost, TTFT, and tok/s for each turn.
- New OllamaCloudProvider with dynamic model discovery and automatic context-limit detection.
- Adds iFlytek Spark and Astron MaaS as supported providers.
- Adds Fireworks AI as a declarative provider.

+12 more

▾ **1 more release in this issue** · 2026-07-13 → 2026-07-14

> v1.42.0 NOTES ↗ CODE ↗ STABLE
>
> Goose v1.42.0 adds Ollama Cloud provider, per-message token/cost stats UI, project-grouped sessions, and Python SDK provider bindings.
>
> └──▷ **GET THIS VERSION**

```
$ git clone --branch v1.42.0 https://github.com/aaif-goose/goose.git
# already have the repo? check out this version:
$ git checkout v1.42.0
```

- Adds OllamaCloudProvider with dynamic model discovery and automatic context-limit detection.
- Adds per-message usage stats in the desktop UI: token counts, cost, time-to-first-token (TTFT), and tokens/sec.
- Adds per-message usage and cost tracking with derived session totals.
- Groups chat sessions by project in the navigation panel.
- Shows project names in the directory-switcher dropdown.

+4 more

WAS THIS USEFUL?  

OpenAI Codex CLI ⓘ rust-v0.145.0-alpha.10

3 RELEASES · 2026-07-13 → 2026-07-14 NOTES ↗ CODE ↗ PRE-RELEASE

Lightweight coding agent that runs in your terminal

Codex CLI alpha adds managed Bedrock login, stabilized memories, MCP OAuth credential pinning, and Windows sandbox level support.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.145.0-alpha.10
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.145.0-alpha.10
```

- Adds managed Bedrock login API for authenticating with AWS Bedrock-hosted models.
- Stabilizes the memories feature flag, making conversation memory generally available.
- Supports MCP OAuth credential store resolution and pinning, with serialized credential refreshes.
- Adds Windows sandbox level configuration propagated through command execution.
- Imports enabled plugins from known marketplaces automatically.

+5 more

▾ 2 more releases in this issue · 2026-07-13 → 2026-07-14

rust-v0.145.0-alpha.9 NOTES ↗ CODE ↗ PRE-RELEASE

Codex CLI adds environment status inspection API and SQLite-backed paginated thread history for faster local reads.

└──▷ GET THIS VERSION

```
$ git clone --branch rust-v0.145.0-alpha.9
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.145.0-alpha.9
```

- New experimental `environment/status` request lets you inspect a configured environment's state (`ready` , `pending` , `disconnected` , or `unknown`) without starting or reconnecting it.
- Adds cursor-based local reads for turn summaries and thread or per-turn items backed by SQLite, enabling paginated thread history with archived-thread and history-mode validation.
- Probes ready remote environments over their existing exec-server connection to report live status.

rust-v0.145.0-alpha.7 NOTES ↗ CODE ↗ PRE-RELEASE

Codex CLI alpha.7 makes GPT-5.6 Sol the default Bedrock model and adds explicit advanced-reasoning selection in the TUI.

└──▷ **GET THIS VERSION**

```
$ git clone --branch rust-v0.145.0-alpha.7
https://github.com/openai/codex.git
# already have the repo? check out this version:
$ git checkout rust-v0.145.0-alpha.7
```

- Sets GPT-5.6 Sol as the default Amazon Bedrock model, prioritizing Sol, Terra, and Luna variants ahead of GPT-5.5 and GPT-5.4.
- Adds explicit advanced reasoning selection in the TUI, making reasoning-level choices visible rather than implicit.
- Automatically omits unsupported `reasoning.summary` parameter for models that lack the capability, including spawned agents using a different model.
- Persists paginated thread items in the local thread store, enabling canonical `ItemCompleted` events to survive across sessions.
- Trusts hooks from newly installed or updated remote workspace plugins automatically after a successful refresh.

+3 more

WAS THIS USEFUL? 👍 👎

Cline ⓘ cli-v3.0.40 NOTES ↗ CODE ↗

Autonomous coding agent as an SDK, IDE extension, or CLI assistant.

Cline CLI v3.0.40 adds a manual API key escape hatch for OAuth providers and clearer ClinePass usage-limit error surfacing.

└──▷ **GET THIS VERSION**

```
$ git clone --branch cli-v3.0.40 https://github.com/cline/cline.git
# already have the repo? check out this version:
$ git checkout cli-v3.0.40
```

- Adds a manual API key entry option in settings for Cline OAuth providers, letting you bypass OAuth and supply a key by hand.
- Surfaces ClinePass usage-limit errors clearly when you hit the plan limit, instead of failing silently.

WAS THIS USEFUL? 👍 👎

AGENT

◆ AI Agent Frameworks

OpenClaw ⓘ v2026.7.1 NOTES ↗ CODE ↗

Your own personal AI assistant. Any OS.

OpenClaw v2026.7.1 adds `openclaw attach` for Claude Code, GPT-5.6/Tencent Hy3/Muse Spark 1.1 support, guarded terminals, and a redesigned Control UI.

└─▷ GET THIS VERSION

```
$ git clone --branch v2026.7.1
https://github.com/openclaw/openclaw.git
# already have the repo? check out this version:
$ git checkout v2026.7.1
```

└─▷ TRY IT

Approve an unknown sender's pairing request so they can interact with the assistant via a connected channel.

```
$ openclaw pairing approve <channel> <code>
```

Run the guided onboarding wizard to set up the gateway daemon and verify connections before saving.

```
$ openclaw onboard --install-daemon
```

- Adds `openclaw attach` command to give Claude Code temporary access to a selected session, enabling tracked Codex delegation and native subagent workflows.
- Supports GPT-5.6 across OpenAI and Codex routes, adds Tencent Hy3 with a complete setup path, and adds Meta Muse Spark 1.1 via the Meta Model API.
- Introduces guarded workspace terminals accessible across web, iOS, and Android.
- Enables scheduled cron jobs to wake only when something changes (change-triggered wake mode).
- Supports pairing remote signed-in browser tabs and safely saving completed downloads from those tabs.

+3 more

WAS THIS USEFUL? 👍 👎

DEPLOY

◆ Local LLM Runtimes

Ollama ⓘ v0.32.0 NOTES ↗ CODE ↗

Get up and running with Kimi-K2.6, GLM-5.1, MiniMax, DeepSeek, gpt-oss, Qwen, Gemma and other models.

Ollama v0.32.0 adds an interactive agent TUI, renames the ChatGPT integration, and warns on deprecated agent models.

└──▷ GET THIS VERSION

```
$ git clone --branch v0.32.0 https://github.com/ollama/ollama.git
# already have the repo? check out this version:
$ git checkout v0.32.0
```

└──▷ TRY IT

Start the new interactive agent to chat, write code, and delegate work — no model name needed.

```
$ ollama
```

Route local model traffic through the ChatGPT desktop app (formerly 'Codex App') integration.

```
$ ollama launch chatgpt
```

- Adds an interactive agent experience: running `ollama` now launches a built-in agent for chat, coding, web search, and delegating real work.
- Adds `--restore` flag to `ollama launch chatgpt` to return to your usual ChatGPT profile.
- Simplifies the `ollama launch` root menu to a curated short list of popular integrations; all others remain accessible via `ollama launch <integration>`.
- Warns before launching older/weaker agent models (CodeLlama, Qwen2.5, Qwen2.5-Coder, Llama 3.x, Mistral, StarCoder, base DeepSeek-R1 tags); use `--yes` to bypass in headless workflows.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 14, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe