THE CYBER TOOLCHAIN

NO. 004

Diff

WHAT VENDORS CHANGED AND DIDN'T ANNOUNCE

PUBLISHED JULY 29, 2026 · WEDNESDAYS

What changed in the docs of the products you run and evaluate.

▸ // HOW THIS ISSUE IS MADE SHOW

▸ // CONTENTS SHOW 64 tools

OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

Maigret

Feedback ⓘ docs update 2026-07-24 DOCS ↗

+ NEW IN THE DOCS maigret.readthedocs.io

Maigret adds QQ and Bilibili numeric ID lookup via `--id-type`, extracting profile metadata from each platform's API. Maigret: Adds `qq_id` identifier type to look up QQ (Tencent) accounts by numeric ID via the Qzone portrait API, extracting nickname and avatar. Maigret now supports filtering site searches by identifier type, including Steam, VK, ORCID, QQ, Bilibili, and more.

Read on maigret.readthedocs.io →

└──▷ DETAILED CHANGES · 3

⇄ Full diff

+ Adds `qq_id` identifier type to look up QQ/Qzone accounts by numeric ID, extracting… ▸

+ Adds `bilibili_id` identifier type to look up Bilibili users by numeric `mid` via the… ▸

+ Adds identifier-type filtering so searches automatically exclude sites whose ID format… ▸

WAS THIS USEFUL? 👍 👎

◆ Password & Credential Cracking

bruteforce-salted-openssl

Feedback ⓘ docs update

DOCS ↗

◆ NEW PAGE github.com

bruteforce-salted-openssl 1.4.1 adds an option to ignore the salt during brute-force attacks.

Read the new page on github.com →

└──▷ DETAILED CHANGES · 1

\+ Adds an option to ignore the salt when brute-forcing OpenSSL-encrypted files.

WAS THIS USEFUL? 👍 👎

◆ Post-Exploitation

SpecterOps BloodHound

Feedback ⓘ docs update

2026-07-24 DOCS ↗

+ NEW IN THE DOCS bloodhound.specterops.io

BloodHound Enterprise gains a native Jira Cloud integration to sync Attack Path findings directly into Jira issues for remediation tracking. BloodHound Enterprise adds native Jira integration for attack path remediation ticketing.

Read on bloodhound.specterops.io →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- \+ New Jira Cloud app (built on Atlassian Forge) automatically synchronizes BloodHound...
- \+ Maps BloodHound Enterprise zones to Jira priorities and sets due dates based on finding priority.
- \+ Filters synchronization by BloodHound Enterprise domains and zones.
- \+ Embeds direct Graph View links in every Jira ticket for in-context investigation.
- \+ Automatically closes Jira tickets when BloodHound Enterprise findings are remediated.
- \+ Supports Jira Service Management request types and incidents for SLA-based remediation tracking.
- \+ Integrates BloodHound Enterprise with Jira to create and track remediation tickets directly from attack path findings.





WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

StepSecurity

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.stepsecurity.io

StepSecurity adds Agent Skills support for developer machines.

Read on docs.stepsecurity.io →

└──▷ DETAILED CHANGES · 1

⇄ Full diff

\+ New Agent Skills capability for developer machines enables automated security skill execution in agentic workflows.

WAS THIS USEFUL? 👍 👎

Portkey

Feedback ⓘ docs update SEEN 2026-07-24 → 2026-07-28

DOCS ↗

+ NEW IN THE DOCS portkey.ai

Portkey forwards request metadata as AWS STS session tags, enabling per-app Bedrock cost attribution in Cost Explorer and CloudTrail. Portkey adds support for configuring custom gateway endpoints for organizations. Portkey adds Prisma AIRS agentic scan controls, soft-deny guardrails, provider-backed model listing, and Continue.dev integration.

Read on portkey.ai →

└──▷ DETAILED CHANGES · 22

⇄ Full diff

- \+ Supports AWS STS session tags for Bedrock ▸
- \+ Clarifies that `model` conditions and `group_by` keys use the request model name (e.g.... ▸
- \+ Supports custom gateway URLs, enabling organizations to configure dedicated endpoints for their Portkey gateway.
- \+ Adds `scan_scope` and `strip_scaffolding` parameters to the Palo Alto Networks Prisma... ▸
- \+ Adds `soft_deny_200` flag on guardrail checks ▸
- \+ `GET /v1/models` now routes through the gateway's provider-backed model listing... ▸
- \+ Anthropic cost attribution now differentiates batch (50% discount), fast, and standard... ▸
- \+ xAI server-side tool invocation costs (file search, web search) are now tracked for cost attribution.
- \+ New integration guide for Continue.dev ▸
- \+ New Admin API endpoints to create, list, and test MCP Server connections for workspace instances.

- New Admin API endpoints to manage SCIM group-to-workspace mappings (create, list...
- New Admin API endpoints to create and list Rate Limits Policies and Usage Limits...
- New Admin API endpoint to rotate existing API keys and retrieve a new key.
- New Admin API endpoints to list and retrieve individual Guardrail configurations.
- New Admin API endpoints for custom model management
- New Admin API endpoints to list and update workspace access permissions and usage limits per integration.
- New Admin API endpoints to create and list Prompt Collections, update prompt metadata, and update prompt version metadata.
- New Skills Registry for creating versioned, team-shared skills usable by AI coding agents via Portkey.
- New guide for converting local STDIO MCP servers to remote Streamable HTTP MCP servers via Portkey's MCP Gateway.
- New integration support for AWS AgentCore, Agno AI, enabling Portkey-powered agents inside Amazon Bedrock and Agno.
- New use-case guide for using private MCP Servers with the Responses API via client-side tool handling.
- New C# (.NET) SDK support for integrating Portkey in .NET applications.

WAS THIS USEFUL? 👍 👎

Openlayer

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.openlayer.com

Openlayer CLI gains data-sources, profile, projects, tests, and update commands; adds tabular ML prediction publishing.

Read on docs.openlayer.com →

└──▷ DETAILED CHANGES · 6

⇄ Full diff

- \+ New `data-sources` CLI command to manage Openlayer data sources directly from the terminal.
- \+ New `profile` CLI command to manage authentication profiles for the Openlayer CLI.
- \+ New `projects` CLI command to manage Openlayer projects from the CLI.
- \+ New `tests` CLI command to export test definitions (goals) for an Openlayer project.
- \+ New `update` CLI command to self-update the Openlayer CLI to the latest version.
- \+ Supports publishing traditional/tabular ML model predictions to Openlayer for... ▸

WAS THIS USEFUL? 👍 👎

graudit

Feedback ⓘ docs update 2026-07-24 DOCS ↗

◆ NEW PAGE github.com

graudit gains JWT rules, SVN repo scanning, commit-log vuln checks, and expanded rulesets across 8+ languages. graudit 3.9 adds JWT and Docker rule sets plus four new misc helper scripts for git, SVN, and serial enumeration. graudit 4.0 adds seventaint.sh PHP taint-flow tracker, 3rd-party JS ruleset, and expanded exec/suppression signatures.

Read the new page on github.com →

└──▷ DETAILED CHANGES · 27

+	Adds JWT detection ruleset for identifying JWT-related vulnerabilities in source code.
+	Enables scanning of SVN repositories by checking out and running rules against them.
+	Supports running rules on every commit in a git repository's history.
+	Adds ability to check for vulnerabilities in commit log messages.
+	Adds detection of SQLi override suppression patterns in .NET code.
+	Expands rulesets for Go, SQL, secrets, .NET, Java, JavaScript, Python, PHP, Ruby, and Scala.
+	Updates Docker rules and test cases with new detection patterns.
+	Adds `giterate` misc script for iterating over git repositories.
+	Adds `snumerate` misc script for serial/sequential enumeration tasks.
+	Adds `svnlog` misc script for working with SVN log output.
+	Adds `svnscan` misc script for scanning SVN repositories.
+	Adds new JWT detection rules.
+	Adds new Docker-related detection rules.

- Adds `seventaint.sh` misc script that performs iterative (up to 7-hop) PHP taint-flow...
- Adds `3partyjs.db` signature database for detecting third-party JavaScript inclusion...
- Expands `exec.db` with cross-language OS-command-execution patterns covering Python...
- Extends suppression rules to recognise `@codingStandardsIgnore` and `# nosec` markers...
- Broadens .NET SQL injection signatures to match named/string format-string placeholders...
- Adds AMPscript injection detection rules.
- Adds rules for detecting dynamic evaluation of 3rd-party JavaScript scripts.
- Adds `seventaint.sh` helper script to the misc collection.
- Adds Ruby rules covering SQL injection, XSS, exec, open redirect, IDOR, mass...
- Expands Python rules with coverage for exec, SSH, Flask, Django, YAML, pickle, file handling, and SQLi patterns.
- Adds PHP suppression support for PHP Code Sniffer and new SQLi rules.
- Adds .NET and Ruby SQL injection detection updates.
- Adds Bandit suppression support.
- Improves secrets detection in XML and adds auth/GitHub-specific secret rules.

WAS THIS USEFUL? 👍 👎

Snyk

Feedback ⓘ changelog · Jul 24, 2026 DOCS ↗

+ NEW IN THE DOCS docs.snyk.io

Snyk launches Snyk Studio (agentic security), Evo AI-SPM platform, Bruno Collection API scanning, and a unified IDE configuration dialog.

Read on docs.snyk.io →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- + Introduces Snyk Studio, an agentic security platform with quickstart guides for 20+ AI...
- + Adds Evo by Snyk, a new AI Security Posture Management (AI-SPM) platform surface with...
- + Launches Agentic Development Security (ADS) within Evo, covering Agent Supply Chain...
- + Adds support for scanning API targets using Bruno Collections in OpenCollection format...
- + Introduces a Unified IDE Configuration Dialog for setting authentication, CLI, trust...
- + Adds Snyk Studio usage analytics and distribution-at-scale capabilities for agentic security deployments.
- + Adds integration coverage for Anthropic's Claude Enterprise under the Cloud AI Platforms security category.

WAS THIS USEFUL? 👍 👎

Snyk Code

Feedback ⓘ changelog · Jul 24, 2026 DOCS ↗

+ NEW IN THE DOCS docs.snyk.io

Snyk Code gains Rule Extensions: define custom sanitizers to reduce false positives in taint-flow analysis without leaving the platform.

Read on docs.snyk.io →

└──▷ DETAILED CHANGES · 5

- + Adds Rule Extensions, letting teams attach custom sanitizer functions to existing Snyk...
- + Supports custom sanitizer definitions per language to reduce false positives in...
- + Enables impact testing via the API to preview how a proposed Rule Extension would...
- + Configures Rule Extensions directly from Group settings in the Snyk Web UI.
- + Introduces dedicated custom-role permissions to control who can manage and test Rule Extensions via the API and Web UI.

WAS THIS USEFUL? 👍 👎

Cloudsmith

Feedback ⓘ changelog · Jul 25, 2026 CHANGELOG ↗

+ NEW IN THE DOCS cloudsmith.com

Cloudsmith CLI gains automatic OIDC auth and Docker credential discovery; cooldown policies expand to Maven packages.

Read on cloudsmith.com →

└──▷ DETAILED CHANGES · 2

+ Introduces a Docker credential helper in the CLI to automatically authenticate to Cloudsmith registries.

+ Extends cooldown policies to Maven packages, enabling supply-chain protection against... ▸

WAS THIS USEFUL? 👍 👎

Veracode

Feedback ⓘ changelog · Jul 28, 2026 CHANGELOG ↗

+ NEW IN THE DOCS docs.veracode.com

Veracode adds CLI `--exclude` flag, DAST custom host-to-IP mappings, EU Package Firewall, enhanced Python scanner, and Android 17 / .NET 10 static analysis support.

Read on docs.veracode.com →

└──▷ DETAILED CHANGES · 9

+	Adds `--exclude` flag to Veracode CLI v2.51.1 to prevent specified Java packages or JAR files from being scanned.
+	Enables custom host-to-IP address mappings for DAST scans when DNS lookup is unavailable or not desired.
+	Enhances Python static scanner with taint tracking, cross-file analysis, and pattern... ▸
+	Adds support for Android 17 in the Static Analysis Engine v2026.07.
+	Enhances support for .NET 10 in the Static Analysis Engine v2026.07.
+	Expands third-party library detection to include Fluxnova.
+	Expands support for pnpm modules to improve dependency resolution in static analysis.
+	Improves JSP and JSF Expression Language modeling with more complete POJO data... ▸
+	Enhances SQL dialect packaging support in Veracode CLI v2.51.1.

WAS THIS USEFUL? 👍 👎

◆ Secrets Detection & Management

GitGuardian SaaS

Feedback ⓘ docs update

2026-07-23 → 2026-07-28 DOCS ↗

+ NEW IN THE DOCS docs.gitguardian.com

GitGuardian roadmap adds Honeytoken multi-cloud/CI/CD/vault support, Slack App with interactive actions, Teams DMs, and an Amazon Kiro integration. GitGuardian Self-Hosted 2026.7.0 adds Public Monitoring, native Gerrit scanning, Smart Notifiers, 9 new detectors, and an MCP server deployment. GitGuardian adds a dedicated Check Runs dashboard page, Bitbucket source health management, perimeter column customization, and bulk source actions.

Read on docs.gitguardian.com →

└──▷ DETAILED CHANGES · 44

⇄ Full diff

- + Adds Endpoint Breach Detection view, shifting endpoint UX toward asset protection and attack detection.
- + Surfaces Non-Human Identity policy breaches (overprivilege, stale identities… ▸
- + Replaces the Slack webhook notifier with a native Slack App that threads incident… ▸
- + Adds interactive Slack Block Kit buttons (Resolve / Ignore) so developers can act on… ▸
- + Delivers incident notifications as Microsoft Teams direct messages to the responsible… ▸
- + Adds a GitGuardian Power for Amazon Kiro with secret-detection skill guidelines, MCP… ▸
- + Expands Honeytoken support beyond AWS to GCP service account JSON keys and Azure AD client secrets.
- + Adds new Honeytoken deception primitives ▸
- + Enables Honeytoken injection into CI/CD runners to detect supply-chain attacks that exfiltrate environment variables.

- Enables planting Honeytokens inside HashiCorp Vault, AWS Secrets Manager, and Azure Key...
- Adds a unified protection coverage dashboard across all asset types
- Introduces an `Attack Detection` incident type that surfaces Honeytoken triggers as...
- Adds Public Monitoring to self-hosted instances (license-gated)
- Adds native Gerrit VCS source with full historical scanning, real-time detection via...
- Adds Smart Notifiers: define per-channel filtering rules so alerts, tickets, or emails are only created for incidents matching severity, validity, secret type, or GitGuardian tag
- GitHub check runs now scan oversized pull requests by cloning the repository branch...
- Adds Gateway API routing
- Adds 9 new detectors (Amadeus OAuth Credentials, Kinde OAuth Credentials, TomTom API...
- Jira Notifier now exposes remediation guidance and detector-specific links as...
- Custom Sources (BYOS) now support a scan-with-validated-detectors-only option.
- Daily analytics job can now write Spark scratch data to a dedicated ephemeral volume...
- Adds opt-in `mcpServer` Helm deployment to run the GitGuardian MCP server in-cluster (currently in beta).
- Incident assignment now auto-grants access to the assignee.
- New dedicated Check Runs page in the dashboard lets security teams browse all GitHub check run results (status, repo, commit SHA, PR, timing), filter by repository/status/date, re-run or skip checks, and jump directly to linked incidents — without switching to GitHub.
- Fine-grained GitHub personal access tokens can now be used to monitor private members...

- Perimeter table now supports column customization, letting users choose which source...
- Bulk actions on perimeter sources now support Monitor, Unmonitor, and Assign Team...
- Historical scans now have their own dedicated tab on the perimeter page for tracking...
- Adds detector for LiteLLM API Key (without host capture).
- Adds detector for Azure SQL Credentials (Assignment).
- Adds detector for Azure Machine Learning keys.
- Adds detector for Azure Video Indexer Key.
- Adds detector for Azure Health Insights Key.
- Adds detector for Azure Fluid Relay Key.
- Adds detector for Apify Proxy Token.
- Adds detector for DashScope API Key (signed/workspace Alibaba Cloud Model Studio / Qwen keys).
- Adds detector for Authress Service Client Access Key.
- Adds detectors for Gemfury Deploy Or Push Token Without Username and Gemfury Full Access Token Without Username.
- Improves recall for Datadog API Key and Snyk Key detectors.
- Adds validity checker for LiteLLM API Key Without Host with custom host support.
- Adds validity checker for Llama Cloud API key.
- Adds validity checker for New Relic APM License Key.
- Adds validity checkers for npm token and npm token (prefixed variant).
- Adds @mention support in incident notes and feedback

WAS THIS USEFUL? 👍 👎

GitGuardian Detection Engine

Feedback ⓘ

changelog · Jul 23, 2026 CHANGELOG ↗

+ NEW IN THE DOCS docs.gitguardian.com Read on docs.gitguardian.com →

└─▷ DETAILED CHANGES · 1

\+ Updated Hume AI API key checker endpoint.

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

Cloudflare

Feedback ⓘ changelog · Jul 23, 2026 CHANGELOG ↗

+ NEW IN THE DOCS developers.cloudflare.com

Cloudflare adds Agents SDK MCP controls, Code Mode direct APIs, Devin Outposts sandboxes, and new WAF rules for Next.js/ColdFusion/WordPress CVEs.

Read on developers.cloudflare.com →

└─▷ DETAILED CHANGES · 7

⇄ Full diff

- \+ Adds `includeMcpTools` option to `@cloudflare/think` to opt out of Think's automatic… ▸
- \+ Agents SDK MCP clients now reuse converted input/output schemas across model turns… ▸
- \+ Adds execute(), search(), and describe() methods to the `@cloudflare/codemode` durable… ▸
- \+ Introduces Devin Outposts ▸
- \+ Deploys new WAF rules covering Next.js DoS (CVE-2026-64641), Next.js SSRF in Server… ▸
- \+ Enhances WAF generic protections against SSRF, Local File Inclusion (LFI), and Cross-Site Scripting (XSS).
- \+ Introduces the Permission Groups API as the replacement for the deprecated Account… ▸

└─▷ BREAKING ON UPGRADE

! The Account Roles API is deprecated and replaced by the Permission Groups API; integrations must obtain Permission Group IDs from the new API and use them in Account Members API policies — legacy Role IDs must be remapped.

! The `PermissionGroup` response replaces the legacy `Role` top-level `description` and `permissions` object (keyed by resource type with edit/read flags) with a `meta` object containing `label` and `scopes`; individual permissions are no longer returned as part of the permission group.

WAS THIS USEFUL? 👍 👎

Wallarm

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.wallarm.com

Wallarm API Discovery adds MCP protocol support alongside documented node version requirements for GraphQL, SOAP, gRPC, and MCP.

Read on docs.wallarm.com →

└──▷ DETAILED CHANGES · 2

⇄ Full diff

+ Supports MCP (Model Context Protocol) discovery, requiring NGINX Node 6.12.0 or Native Node 0.25.0.

+ Documents minimum node versions for API Discovery across all supported protocols ▸

WAS THIS USEFUL? 👍 👎

dirsearch

Feedback ⓘ docs update DOCS ↗

◆ NEW PAGE github.com

dirsearch v0.4.3 adds SQLite reports, progress save/resume, client cert support, and built-in web crawler.

Read the new page on github.com →

└──▷ DETAILED CHANGES · 9

+ Automatically detects HTTP or HTTPS URI scheme when no scheme is provided in the target URL.
+ Adds SQLite as a new report output format.
+ New option to overwrite unwanted extensions with a selected set of extensions.
+ New option to view redirect history when following redirects.
+ New option to crawl web paths discovered in HTTP responses.
+ Saves all HTTP traffic to the log file for offline review.
+ Adds capability to save scan progress and resume it later.
+ Supports client certificate authentication.
+ Configurable maximum log file size via configuration.

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

ElcomSoft

Feedback ⓘ changelog · Jul 23, 2026 CHANGELOG ↗

+ NEW IN THE DOCS elcomsoft.com

Elcomsoft Phone Breaker 11.03 adds universal binary for macOS and restores SMS-based iCloud two-factor authentication.

Read on elcomsoft.com →

└──▷ DETAILED CHANGES · 1

\+ Ships as a universal binary for macOS, running natively on both Apple Silicon and Intel Macs.

└──▷ BREAKING ON UPGRADE

! The pre-login 2FA status check is removed, as Apple no longer supports it.

WAS THIS USEFUL? 👍 👎

◆ Reverse Engineering

HyperDbg

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.hyperdbg.org

HyperDbg adds `ucpuid` command to execute CPUID in the debuggee and new scripting language data types & operators docs.

Read on docs.hyperdbg.org →

└──▷ DETAILED CHANGES · 2

⇄ Full diff

+	New `ucpuid` command executes a CPUID instruction directly in the debuggee context.
+	Scripting language gains documented data types and operators for use in HyperDbg scripts.

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Firewalls & Network Defense

Rspamd

Feedback ⓘ docs update 2026-07-22 → 2026-07-26 DOCS ↗

+ NEW IN THE DOCS docs.rspamd.com

Rspamd 4.1.3 adds fuzzy hash diagnostics API, ClickHouse export, ARF enrichment, SSRF protection for lua_http, and a jQuery-free WebUI. Rspamd 4.1.2 adds composite Lua conditions, static_embed neural provider, neural training freeze, external rspamadm command discovery, and WebUI Tabulator migration. Rspamd 4.1.2 adds sender-identity preservation for DMARC/SPF, composite Lua conditions, and WebUI Tabulator migration.

Read on docs.rspamd.com →

└──▷ DETAILED CHANGES · 30

⇄ Full diff

- \+ Adds structured fuzzy match results and a diagnostics API
- \+ Adds `rspamadm fuzzy_hash` command to compute a message's fuzzy hashes per configured...
- \+ Adds `rspamadm control fuzzyhash <128-hex-digest>` per-hash storage introspection...
- \+ Adds configurable fuzzy probability weight curve via `prob_bias` and `prob_power`...
- \+ Adds persistent shingle sets in the Redis fuzzy backend (`S` field on every ADD)...
- \+ Adds unkeyed client statistics
- \+ Adds ClickHouse fuzzy match export
- \+ Adds annotated `X-Rspamd-Fuzzy` milter header built from structured fuzzy results...
- \+ Adds `forbid_local` option to rspamd_http.request() to block SSRF via loopback...
- \+ Adds ARF report enrichment in `lua_feedback_parsers`
- \+ WebUI is rewritten to remove jQuery entirely, replacing it with native DOM and `XMLHttpRequest`.

+ Replaces Font Awesome SVG-with-JS (~900 KB) with a local 35-glyph SVG sprite.

+ Adds composite Lua conditions

+ Introduces `policy = "implicit_allow"` in settings `apply` blocks, allowing...

+ Adds `static_embed` neural provider

+ Adds `train.forced_learn_minimal_scan` neural training option that installs a prefilter...

+ Adds `train.frozen` neural training option that halts automatic training and vector...

+ Adds task:disable_all_symbols([skip_mask]) Lua binding.

+ Enables external `rspamadm` sub-command discovery from a `rspamadm.d` drop-in directory...

+ Supports supplying the controller password via environment variable for non-interactive...

+ Adds `--symbol-details` flag to `rspamadm configdump`, reporting a `flags` array per...

+ Migrates all WebUI tables from FooTable to Tabulator, adding per-column header filters...

+ Exposes `aliased` and `original` email-address flags to Lua and adds the `orig` address...

+ Preserves sender identity through DMARC/SPF processing pipelines.

+ Supports composite Lua conditions for more expressive rule authoring.

+ Migrates the WebUI to the Tabulator library for improved table rendering.

+ Invalid selectors now fail configuration load with an error pointing at the offending...

+ Glob map patterns are now compiled anchored (`^(?:...)$`) at load time, closing a...

+ Symbols carrying the `explicit_enable` flag are now strictly gated

+ `lua_cryptobox` secretbox now correctly zero-pads short nonces to 24 bytes, producing...

└─▷ BREAKING ON UPGRADE

! The WebUI drops jQuery entirely and deletes the vendored jQuery build; any local customizations or extensions depending on jQuery or the `$.fn` API will break.

! The `modalDialog` backdrop attribute is renamed from its previous name to `data-bs-backdrop` (Bootstrap 5 native); custom WebUI code referencing the old attribute will lose the static-backdrop behaviour.

! Font Awesome SVG-with-JS is removed in favour of a local SVG sprite; any custom markup or extensions referencing Font Awesome JS APIs or its CSS classes outside the automated `<i class="fas fa-name">` replacement sweep will stop rendering icons.

! The old zero-anchored fuzzy probability weight curve (sqrt(prob)) is not preserved; deployments relying on the previous scoring behaviour for non-exact fuzzy matches will see different scores after upgrade.

! `HAVE_ED25519` no longer gates libsodium Ed25519 code in the DKIM path; builds that previously worked around missing OpenSSL Ed25519 support via compile-time flags may need configuration review.

WAS THIS USEFUL? 👍 👎

Palo Alto Networks

Feedback ⓘ changelog · Jul 24, 2026

DOCS ↗

+ NEW IN THE DOCS docs.paloaltonetworks.com

AI Runtime Security adds tool chaining attack detection in agent scans, Azure SLR support, and updated vCPU capacity.

Read on docs.paloaltonetworks.com →

└──▷ DETAILED CHANGES · 3

⇄ Full diff

+	Adds Tool Chaining Attack detection capability within Agent Scans for AI runtime security.
+	Adds Security Lifecycle Review (SLR) support for Azure environments.
+	Updates vCPU support limits for AI Runtime Security deployments.

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

Sysdig Secure

Feedback ⓘ changelog · Jul 23, 2026 CHANGELOG ↗

+ NEW IN THE DOCS docs.sysdig.com

Sysdig Secure adds multi-bucket Custom Storage support and a redesigned Posture Overview & Findings experience.

Read on docs.sysdig.com →

└─▷ DETAILED CHANGES · 4

- + Adds Custom Storage: connect multiple S3 or S3-compatible buckets (MinIO, Google Cloud Storage, etc.) for use across Captures, Response Actions, and Rapid Response ▸
- + Supports AWS access keys, AWS role delegation (AssumeRole), and S3-compatible endpoints... ▸
- + Introduces a new Posture Overview page surfacing passing scores, 30-day trends, and... ▸
- + Introduces a new Posture Findings workspace with filtering, grouping, and remediation... ▸

└─▷ BREAKING ON UPGRADE

! The previous single shared S3 Capture Storage configuration is replaced by the new Custom Storage system; existing Capture Storage settings will need to be reconfigured under Data Sources > Storage.

WAS THIS USEFUL? 👍 👎

Prowler

Feedback ⓘ docs update 2026-07-24 DOCS ↗

◆ NEW PAGE docs.prowler.com

Prowler adds Claude Code integration via MCP Server and a Prowler Plugin with guided cloud compliance workflows. Prowler adds an MCP Server for AI agent integration and launches a dedicated MSP/MSSP multi-tenant offering.

Read the new page on docs.prowler.com →

└──▷ DETAILED CHANGES · 7

- \+ New Prowler MCP Server at `https://mcp.prowler.com/mcp` enables Claude Code to query...
- \+ New Prowler Plugin for Claude Code bundles official skills, including...
- \+ Compliance triage skill supports two modes
- \+ Plugin manages API key storage securely (macOS keychain or...
- \+ MCP Server connection supports `--scope user` to make Prowler tools available across...
- \+ New Prowler MCP Server enables AI agents (Claude, Cursor, VS Code/GitHub Copilot...
- \+ New Prowler for MSPs and MSSPs tier adds partner organization management, customer...

WAS THIS USEFUL? 👍 👎

◆ Runtime Security

Cilium tetragon

Feedback ⓘ docs update 2026-07-24 DOCS ↗

◆ NEW PAGE tetragon.io

Tetragon gains persistent gRPC policies: tracing policies survive agent restarts with zero enforcement gaps via BPF handoff. Tetragon now supports persistent gRPC policies that survive restarts and can be restored automatically. Tetragon adds in-kernel CEL expression argument filtering and uprobe override actions with register manipulation support.

Read the new page on tetragon.io →

└──▷ DETAILED CHANGES · 11

+	New `--persist-grpc-policies` flag enables saving and restoring tracing policies... ▸
+	New `--persist-grpc-policies-dir` flag selects the directory used as the policy store (default: `/var/run/tetragon/grpc-policies`).
+	Combined with `--keep-sensors-on-exit` and `--release-pinned-bpf=false`, Tetragon performs a zero-gap BPF handoff ▸
+	Policy lifecycle operations (`tetra tracingpolicy add/delete/enable/disable/set-mode`)... ▸
+	Atomic failure handling ensures the running policy and its stored record stay consistent ▸
+	Stored policies use a per-policy JSON record format keyed by... ▸
+	Adds persistent gRPC policies ▸
+	New `CelExpr` argument filter enables specifying Common Expression Language (CEL)... ▸
+	Uprobe override action now supports redirecting traced user-space symbols to a new... ▸
+	Adds `binaryDigests` field to uprobe tracing policies, allowing policies to validate a target binary's hash before attaching ▸

+ Supports sha1, sha256, sha384, sha512, and ELF build-id (`.note.gnu.build-id`) digest types for binary verification.

└─▷ **BREAKING ON UPGRADE**

! `--release-pinned-bpf` defaults to `true` ; continuous enforcement across restarts requires explicitly setting `--release-pinned-bpf=false` , otherwise the previous BPF tree is removed at startup before replacement policies load.

WAS THIS USEFUL? 👍 👎

Docker Sandboxes

Feedback ⓘ docs update 2026-07-24

DOCS ↗

+ NEW IN THE DOCS docs.docker.com

Docker Sandboxes org admins can now add a custom support message shown when governance policies block sandbox actions. Docker Sandboxes 0.37.0+ adds ChatGPT desktop app integration via SSH, letting Codex run inside an isolated sandbox instead of on the host. Docker Sandboxes now supports connecting Claude Desktop to a remote sandbox over SSH for isolated AI agent execution.

Read on docs.docker.com →

└──▷ DETAILED CHANGES · 16

⇄ Full diff

- + Adds configurable support message (up to 500 characters) displayed to members when a...
- + Supports connecting the ChatGPT desktop app to a Docker Sandbox over SSH so OpenAI...
- + Adds a Codex sandbox template that pre-installs the `codex` command required by the ChatGPT app's remote server.
- + Enables Claude Desktop to run Claude Code inside a Docker Sandbox over SSH, keeping...
- + Adds SSH connection workflow in Claude Desktop
- + Provides Windows-specific troubleshooting guidance for SSH connection timeouts caused...
- + Connects the Cursor editor to a Docker Sandbox over Remote-SSH, keeping the editor on...
- + Supports connecting VS Code to a running sandbox via the Remote-SSH extension, so...
- + New `sbx setup ssh` command configures SSH access to sandboxes, writing a managed block...

+	Sandboxes are now reachable as SSH hosts via `<name>.sbx` naming, enabling remote... ▸
+	SSH connections route through the daemon's local socket (Unix domain socket on macOS/Linux, named pipe on Windows) ▸
+	Environment variable forwarding via `SendEnv *` is supported, filtered by a daemon-side... ▸
+	Adds `sbx skills import` command to copy agent skills (Claude Code, Codex, Copilot... ▸
+	Adds `--dry-run` flag to `sbx skills import` to preview which skills would be copied without committing them to the store.
+	Adds `--no-share-skills` flag to `sbx run` to create a sandbox that opts out of the... ▸
+	Enables connecting VS Code, Cursor, and other editors/apps to a Docker Sandbox over SSH.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ Threat Intelligence

OpenCTI

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.opencti.io

OpenCTI adds `app:uri_deny_list` config option to block specific URIs at the application level.

Read on docs.opencti.io →

└──▷ WHAT'S NEW IN THE DOCS ▸

WAS THIS USEFUL? 👍 👎

Feedly Threat Intelligence

Feedback ⓘ

changelog · Jul 27, 2026 | 2026-07-22 → 2026-07-27 | CHANGELOG ↗

+ NEW IN THE DOCS feedly.com

Feedly Ask AI gains SPL query generation and an improved threat actor campaign detection model alongside KQL support. Feedly's Vulnerability Intel Agent now ingests Apple security releases in minutes, with CVE filtering by exploitation, product, and patch policy. Feedly Threat Intelligence adds Apple security release enrichment and triage in the Vulnerability Intel Agent.

Read on feedly.com →

└──▷ DETAILED CHANGES · 10

- + New Ask AI model tuned specifically for threat actor campaign detection.
- + Adds SPL (Splunk Processing Language) hunting query generation to Ask AI, complementing existing KQL support.
- + Improves MITRE ATT&CK tagging accuracy in Ask AI results.
- + Ingests each Apple security release into the Vulnerability Intel Agent within minutes of publication.
- + Supports filtering Apple release CVEs by exploitation activity (exploited, PoC, weaponized, CISA KEV).
- + Enables product-level filtering to scope CVEs to only the Apple products in your environment.
- + Supports CVSS and EPSS threshold filters to enforce patch-now policies and SLA-driven remediation.
- + Adds an Alerts capability to notify teams when new CVEs in a deployed Intel Agent match configured filters.
- + Provides a customizable output table with reorderable, show/hide columns for each CVE enrichment field.
- + Enables enrichment and triage of Apple security releases directly within the Vulnerability Intel Agent.

WAS THIS USEFUL?  

◆ Detection Engineering

Tenzir

Feedback ⓘ docs update 2026-07-22 → 2026-07-25 DOCS ↗

◆ NEW PAGE docs.tenzir.com

Tenzir v6.8.1 adds GMT/UTC/UT timezone parsing support and warnings for unparsable timestamps in time(). Tenzir v6.8.0 adds a Splunk search input operator and improves ClickHouse batching and JSON column support. Tenzir v6.8.0 adds a Splunk search input for ingesting data from Splunk.

Read the new page on docs.tenzir.com →

└──▷ DETAILED CHANGES · 11

⇄ Full diff

- + Supports zero-offset timezone names (`GMT` , `UTC` , `UT`) in timestamp parsing, enabling...
- + Adds automatic type detection for `GMT` / `UTC` / `UT` `-suffixed` values (e.g., in CSV...
- + The time() function now emits a warning with the offending value when a string cannot...
- + Adds a Splunk search input operator, enabling Tenzir nodes to pull data directly from Splunk searches.
- + New `from_splunk` operator runs bounded searches against a Splunk Search Head and emits...
- + The `to_clickhouse` operator now internally re-batches events before inserting...
- + The `to_clickhouse` operator can now write `string` values directly into a ClickHouse...
- + Platform connection logs now include the workspace name and node ID when a node connects to the Tenzir Platform.
- + New Splunk search input enables pulling data from Splunk into Tenzir pipelines.
- + `to_clickhouse` re-batches events before insert for higher throughput and supports writing directly into JSON columns.

+ Workspace and node ID are now included in platform connection logs for better traceability.

└─▷ **BREAKING ON UPGRADE**

! Values like `"2026-07-21 13:55:59 GMT"` that previously stayed as strings are now automatically recognized as timestamps during type detection (e.g., when reading CSV files), which may change pipeline behavior for workflows relying on those values being strings.

WAS THIS USEFUL? 👍 👎

◆ Security Data Pipeline

Cribl

Feedback ⓘ docs update 2026-07-22 → 2026-07-25 DOCS ↗

+ NEW IN THE DOCS docs.cribl.io

Cribl LLM Observability adds Mistral AI support via OpenTelemetry instrumentation. Cribl AI gains an MCP server for external agent access and Guard recommendations for actionable detection guidance.

Read on docs.cribl.io →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- + Supports instrumenting Mistral AI with OpenTelemetry to send telemetry to Cribl Stream and Cribl Search.
- + New MCP server lets external AI clients (Cursor, Claude Code, Codex) connect to Cribl...
- + Guard recommendations surface a suggested action (create a rule, mark mitigated, or...
- + MCP Integrations setting allows Cribl to call tools from an approved list of external agents via MCP.
- + Web Search option enables a Cribl agent to search the web for information during Search investigations.
- + Bring Your Own Model (BYOM) support lets operators route Cribl AI through their own...
- + AI feature entry points remain visible and surface a actionable error message when a...

WAS THIS USEFUL? 👍 👎

◆ SIEM

Google SecOps

Feedback ⓘ docs update 2026-07-23 → 2026-07-24

DOCS ↗

◆ NEW PAGE cloud.google.com

Google Unified Security adds Chrome Enterprise threat detection, multi-cloud CDIR, and AI Protection for securing AI workloads. Google SecOps introduces Security Tokens for metering agentic consumption, and announces legacy SIEM API deprecation timeline. Google SecOps adds Advanced Filtering with dynamic YARA-L query variables in dashboards, plus Security Tokens for agentic consumption metering.

Read the new page on cloud.google.com →

└──▷ DETAILED CHANGES · 14

⇄ Full diff

+ Adds Chrome Enterprise Premium integration with curated detections enriched by Safe...

+ Adds dedicated Google SecOps dashboards for Chrome security events and anomalies to...

+ Enables automated SOAR playbook response actions on Chrome Enterprise

+ Adds Cloud Detection, Investigation, and Response (CDIR) capability spanning Google...

+ Adds Cloud Asset Inventory collection that flows multi-cloud asset metadata (AWS...

+ Supports natural language query syntax alongside existing Yara-L and raw log search for...

+ Integrates AI Protection into Security Command Center Enterprise (SCC-E), providing...

+ Adds Model Armor for model- and cloud-agnostic protection against data loss, brand...

+ Adds Agentic AI Triage and Investigation for automatic triage and investigation of security alerts.

+ Adds Advanced Filtering in dashboards (Public Preview) ▸

+ Token values can be generated dynamically from YARA-L query results or entered as a static manual list.

+ Customizable prefix/suffix wrappers on token values enable advanced patterns such as... ▸

+ Multi-select support for token variables allows combining multiple values in a query... ▸

+ Introduces Security Tokens for metering agentic consumption within Google SecOps... ▸

WAS THIS USEFUL? 👍 👎

Exabeam

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.exabeam.com

Exabeam Outcomes Navigator adds support for the OWASP Top 10 for Agentic Applications framework.

Read on docs.exabeam.com →

└──▷ DETAILED CHANGES · 1

⇄ Full diff

+ Supports the OWASP Top 10 for Agentic Applications framework, enabling practitioners to... ▸

WAS THIS USEFUL? 👍 👎

Elastic Security Labs

Feedback ⓘ docs update DOCS ↗

◆ NEW PAGE elastic.co

Elastic Security v9.4 adds Entity Analytics Watchlists to inject organizational risk context directly into entity risk scoring.

Read the new page on elastic.co →

└──▷ DETAILED CHANGES · 4

- \+ New Entity Analytics Watchlists let teams create named, weighted lists of users, hosts, and services that feed directly into the platform's risk scoring pipeline
- \+ Watchlist memberships compound with alert activity, asset criticality, and behavioral...
- \+ Supports both manual curation and automated population via API, enabling integrations...
- \+ Allows creation of allow-list watchlists to dampen scores for known-safe entities...

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

Corellium

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS support.corellium.com

Corellium 7.12 adds Metal graphics support, MCP AI integration, Android KASAN/HWASAN debugging, PongoOS pre-boot, and folder downloads.

Read on support.corellium.com →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- + Adds initial Apple Metal graphics framework support via software-based implementation...
- + Introduces Model Context Protocol (MCP) Server integration, allowing AI-powered tools...
- + Adds Android Kernel Address Sanitizer (KASAN) and Hardware-Assisted Address Sanitizer...
- + Enables pre-booting supported Apple virtual devices directly into PongoOS before...
- + Supports downloading entire folders and nested sub-folder structures from virtual...
- + Adds iOS/iPadOS 26.5.2, 26.6.0 betas 2–4, and 27.0.0 betas 1–3 (Falcon Premium) platform support.
- + Updates Frida framework integration to support the latest Frida releases.

WAS THIS USEFUL? 👍 👎

◆ SOAR

Tines

Feedback ⓘ changelog · Jul 27, 2026 CHANGELOG ↗

+ NEW IN THE DOCS tines.com

Tines 42.2.0 adds API key creation restrictions and template-based case creation via API.

Read on tines.com →

└──▷ DETAILED CHANGES · 2

+	Adds the ability to restrict which users can create API keys.
+	Enables creating cases from a template via the API.

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

runZero

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS help.runzero.com

runZero now displays Purdue levels for assets sourced or enriched from Dragos integration

Read on help.runzero.com →

└──▷ WHAT'S NEW IN THE DOCS ▸

WAS THIS USEFUL? 👍 👎

Axonius

Feedback ⓘ docs update 2026-07-24 → 2026-07-27 DOCS ↗

+ NEW IN THE DOCS docs.axonius.com

Axonius 9.0 introduces a redesigned grouped navigation with expandable menu groups replacing the previous icon-based side menu. Axonius Users page gains a Preferred Last Seen field showing the most recent last_seen timestamp across all adapters.

Read on docs.axonius.com →

└──▷ DETAILED CHANGES · 5

+	New grouped navigation experience in v9.0 organizes all side-menu items into expandable... ▸
+	Cases and Case Sets are now accessible directly from the new Action Center group in the side menu.
+	Activity Log and Nodes are now accessible from the new System group in the side menu.
+	Monitoring page gains a blue notification dot on its side-menu icon when new alerts appear, cleared on page visit.
+	Adds Preferred Last Seen aggregated date field on the Users page, surfacing the most... ▸

WAS THIS USEFUL? 👍 👎

Surface Command

Feedback ⓘ docs update 2026-07-24 DOCS ↗

+ NEW IN THE DOCS docs.rapid7.com

Surface Command adds AI-generated asset summaries covering identity, vulnerabilities, mitigations, and business context. Surface Command: Caches AI summaries for faster repeat access and automatically regenerates them when new data is ingested. Surface Command: Enables practitioners to copy the full formatted AI summary to the clipboard for use in reports or incident notes.

Read on docs.rapid7.com →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

+	Adds AI Summary panel on asset detail pages that provides a concise overview of... ▸
+	AI summaries are generated on first open and cached for faster subsequent access, with... ▸
+	Enables one-click copy of the full formatted AI summary to clipboard from the General tab.
+	Adds thumbs-up/thumbs-down feedback form on AI summaries, allowing practitioners to rate and annotate summary quality ▸
+	Enables one-click copy of the full AI summary (with formatting) to clipboard for use in reports or tickets.
+	Supports thumbs-up/thumbs-down inline feedback on AI summaries with free-text context, submittable multiple times per asset.
+	Supports thumbs-up/thumbs-down feedback submission directly from the AI Summary section to rate and improve summary quality.

WAS THIS USEFUL? 👍 👎

Intruder

Feedback ⓘ changelog · Jul 27, 2026 CHANGELOG ↗

+ NEW IN THE DOCS feedback.intruder.io

Intruder extends Azure cloud scans to cover Microsoft 365 configuration risks across Entra, Exchange, SharePoint, and Teams.

Read on feedback.intruder.io →

└──▷ DETAILED CHANGES · 3

- \+ Adds Microsoft 365 configuration risk scanning (Entra ID, Exchange Online, SharePoint...
- \+ Surfaces M365 identity, email, and collaboration configuration risks automatically for existing Azure integration users.
- \+ Enables full M365 check coverage by updating the Azure integration's permissions.

WAS THIS USEFUL? 👍 👎

Censys

Feedback ⓘ docs update 2026-07-28 DOCS ↗

+ NEW IN THE DOCS docs.censys.com

Censys launches a hosted Adversary Investigation MCP server, giving AI agents (Cursor, Claude Code, Continue.dev) direct access to threat-hunting APIs. Censys Platform adds OAuth 2 Connected Apps management, letting users review and revoke third-party access to Censys APIs.

Read on docs.censys.com →

└──▷ DETAILED CHANGES · 4

⇄ Full diff

- \+ New hosted Adversary Investigation MCP server at... ▸
- \+ Supports OAuth and HTTP header authentication for integrating the MCP server with tools... ▸
- \+ OAuth connections can be managed from Account Settings > Personal Settings > Connected Applications.
- \+ New Connected Apps page in Account Settings lets users audit and revoke OAuth 2 applications ▸

WAS THIS USEFUL? 👍 👎

Rapid7 Surface Command

Feedback ⓘ

changelog · Jul 28, 2026 DOCS ↗

+ NEW IN THE DOCS docs.rapid7.com

Surface Command adds AI asset summaries in ASM and three new connectors: Adaptive Security, Avigilon Alta, and Halcyon.

Read on docs.rapid7.com →

└──▷ DETAILED CHANGES · 7

- + New AI-generated asset summaries in the Attack Surface Management Asset Details view...
- + New Adaptive Security connector imports users and groups from the security awareness training platform into Surface Command.
- + New Avigilon Alta connector integrates Users, Access Groups, ACUs, Readers, and Sites...
- + New Halcyon connector imports endpoint assets, tenant organizations, deployment groups...
- + Microsoft SQL connector adds a generic import feed with configurable queries via a new...
- + CyberArk Endpoint Privilege Manager connector migrates to the new Get Endpoints API...
- + Vector Command now requires service agreement acknowledgment before initiating testing.

└──▷ BREAKING ON UPGRADE

! CyberArk Endpoint Privilege Manager connector migrates from the deprecated GetComputers API to the new Get Endpoints API and introduces the `CyberArkEpmComputer2` type — existing workflows relying on the old API or type may need to be updated.

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

Brinqa

Feedback ⓘ docs update SEEN 2026-07-24 DOCS ↗

+ NEW IN THE DOCS docs.brinqa.com

Brinqa v12 introduces AI Agents for natural-language querying, CVE exploration, and autonomous ownership attribution. BrinqaIQ adds MCP integration so AI clients like Claude Desktop, GitHub Copilot, and Goose can query Brinqa data, generate BQL, and manage automations. Brinqa launches a new BQL API replacing the legacy GraphQL API, enabling programmatic access to the data warehouse via async queries.

Read on docs.brinqa.com →

└──▷ DETAILED CHANGES · 16

⇄ Full diff

+ Adds a user-facing chat agent with three tools ▸

+ Adds an Attribution Agent that autonomously infers Remediation Owner, Business Owner... ▸

+ New MCP server integration exposes BrinqaIQ capabilities ▸

+ Supports natural-language BQL query generation and direct BQL execution with paginated... ▸

+ Automation lifecycle control (launch, resume, cancel, status check) and... ▸

+ Docs Assistant tool lets connected AI clients search and retrieve content from Brinqa Platform documentation inline.

+ CVE Explorer tool enables connected AI clients to look up CVE details, severity... ▸

+ Supports Claude Desktop, GitHub Copilot in VS Code, Goose, and Open WebUI as tested MCP... ▸

+ API token-based authentication ensures all MCP calls inherit the user's existing RBAC... ▸

+ New BQL API (`POST /v1/api/bql`) replaces the legacy GraphQL API, providing... ▸

+ Supports asynchronous two-step query workflow ▸

+ Introduces two query modes

+ Projection mode supports nested relationship projections and wildcards, enabling...

+ Cursor-based pagination allows retrieval of large result sets up to 10,000 rows per...

+ New API token authentication system (`ApiKey` scheme with `brq_` `-prefixed` tokens) tied...

+ New IONIX connector ingests Action Item, Action Item Definition, Cloud Asset, Domain...

WAS THIS USEFUL? 👍 👎

OpenCVE

Feedback ⓘ docs update 2026-07-27 DOCS ↗

◆ NEW PAGE docs.opencve.io

OpenCVE adds Alerts API endpoints to list and retrieve alerts within a report. OpenCVE launches API v2 with read/write access, granular token scopes, and full vulnerability workflow management.

Read the new page on docs.opencve.io →

└──▷ DETAILED CHANGES · 8

+	New `GET /api/reports/<link>/alerts` endpoint lists all alerts for a given report, with pagination support.
+	New `GET /api/reports/<link>/alerts/<id>` endpoint retrieves full details of a specific... ▸
+	New REST API v2 at `https://app.opencve.io/api/v2/` adds write capabilities alongside... ▸
+	Supports bulk subscription replacement via a single PUT request, allowing teams to sync... ▸
+	Introduces organization API tokens with granular scopes (e.g., `catalog:read` ... ▸
+	Interactive Swagger UI at `https://app.opencve.io/api/v2/docs/` lets practitioners... ▸
+	Structured JSON error responses now include machine-readable `code` fields (e.g.... ▸
+	Paginated results support a configurable `page_size` parameter (up to 100 items) for... ▸

WAS THIS USEFUL? 👍 👎

defectdojo

Feedback ⓘ docs update 2026-07-27 DOCS ↗

◆ NEW PAGE docs.defectdojo.com

DefectDojo Pro gains Sensei: AI-powered scan-and-fix that opens remediation PRs on GitHub repositories. DefectDojo Pro adds 20+ new findings connectors, a Linear integrator, per-assignment push filters, and a redesigned feature flags system.

Read the new page on docs.defectdojo.com →

└──▷ DETAILED CHANGES · 18

+	New Sensei AI feature scans GitHub repositories and imports results as findings into DefectDojo Pro.
+	Enables LLM-generated pull requests that remediate findings, using a preview-first...
+	Supports triggering fixes from the findings table, from staged auto-fix candidates, or via a `/fix` comment on a pull request.
+	Adds findings connectors for Rapid7 InsightAppSec, Cobalt.io PtaaS, Sonatype IQ (Nexus...
+	Adds a ServiceNow CMDB asset connector for syncing asset inventory.
+	Registers the Intigriti bug bounty connector and the runZero asset connector in the Pro UI.
+	Adds a Linear integrator for pushing findings directly to Linear.
+	Enables requesting a new connector directly from the cloud UI.
+	Adds per-assignment push filters on integrator assignments, allowing minimum severity...
+	Introduces a cloud dispatch guard, retroactive re-staging of auto-fixes, and a per-row actions menu in the findings list.
+	Redesigns feature flags into a two-tier, metadata-driven system with a dedicated Feature Flags admin page.
+	Adds a configurable OIDC username claim with hardened SSO user creation.

+	Introduces `DD_EDITABLE_MITIGATED_DATA` setting to control whether mitigation data is editable.
+	CrowdStrike Spotlight connector now derives its severity floor from structured sync filters.
+	Export options now prefill from the active table preference; AI menu flattened into...
+	Scan-import cleanup now streams files and fails loudly on error.
+	CVSS and EPSS columns now expose numeric filter operators in the findings table.
+	Metric colors in the Vue UI are now configurable per instance.

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Secure Access (VPN / SASE / ZTNA)

Progress ShareFile

Feedback ⓘ changelog · Jul 26, 2026

2026-07-22 → 2026-07-26 CHANGELOG ↗

+ NEW IN THE DOCS docs.sharefile.com

ShareFile adds a Tasks Workspace for centralized management of Request Lists and Forms across all projects. ShareFile Request Lists now support comments for collaborator communication. Progress ShareFile: Adds the ability to leave comments on Request List items, enabling collaborators to communicate directly within a file request.

Read on docs.sharefile.com →

└──▷ DETAILED CHANGES · 25

+	New Tasks Workspace provides a centralized location to view and manage work items ▸
+	AI-powered Request List generation (Beta) enables users to create Request Lists using AI assistance.
+	Adds the ability to leave comments on Request List items to facilitate in-context communication with collaborators.
+	Adds Forms Notifications, enabling alerts tied to form activity within ShareFile.
+	New Request Lists feature replaces legacy Request List with full lifecycle management ▸
+	Supports creating Request Lists from blank, from a template, or using AI-powered generation (Beta).
+	Adds Request List templates ▸
+	Adds ID field support within Request List items.
+	Adds due date management and automated due date reminders for Request Lists.
+	Adds granular notifications per Request List, including configurable filters.
+	Adds Activity Report generation for individual Request Lists.

- New Forms feature enables structured data collection with blank or template-based creation.
- Forms support conditional logic to show or hide fields based on responses.
- Forms include auto-save of respondent progress.
- Supports sharing Forms, sending Forms for resubmission, and exporting individual form responses.
- Save Forms as reusable templates.
- Adds Request Lists with full lifecycle management
- Supports Request List due dates with automated due-date reminders and configurable notifications.
- Enables per-Request-List filters and activity report generation for audit and tracking purposes.
- Introduces ID fields as addable items within a Request List.
- Adds AI-powered Request List generation (Beta) to auto-create item checklists from a prompt.
- Introduces Forms with blank and template creation, conditional logic, auto-save progress, and resubmission workflows.
- Supports exporting form responses and reviewing/approving submitted forms.
- Adds Form and Request List template libraries with save-as-template capability for reuse.
- Provides a legacy Request List read-only mode and migration FAQ to guide transition to the new Request Lists experience.

WAS THIS USEFUL? 👍 👎

DNSFilter

Feedback ⓘ changelog · Jul 24, 2026 CHANGELOG ↗

+ NEW IN THE DOCS feedback.dnsfilter.com

DNSFilter redesigns the Query Log with multi-select filters, cross-org switching, and URL-persistent views, plus live local domain sync in the macOS client.

Read on feedback.dnsfilter.com →

└──▷ DETAILED CHANGES · 8

- + Redesigned DNS Query Log with a top-level filter bar supporting multi-select across…
- + MSP admins can now toggle between organizations directly from the Query Log without…
- + Introduced a custom timeline picker in the Query Log to narrow search windows down to the second.
- + Active Query Log filters now persist in the URL, enabling bookmarking and sharing of specific filtered views.
- + New Query Log data columns added
- + Any page in the app can now be set as the default landing page upon login.
- + Live local domain and resolver sync
- + Automatic Registration toggle for Mobile Agent now displays its 7-day duration and explicit end date at a glance.

└──▷ BREAKING ON UPGRADE

! Starting with macOS Roaming Client v2.4.4, macOS 13 Ventura or later is required; macOS 12 Monterey is no longer supported.

WAS THIS USEFUL? 👍 👎

Firezone

Feedback ⓘ docs update DOCS ↗

◆ NEW PAGE firezone.dev

Firezone introduces single-owner Gateway tokens with rotation, revocation, and REST API management.

Read the new page on firezone.dev →

└──▷ DETAILED CHANGES · 4

- \+ Adds single-owner Gateway tokens ▸
- \+ Supports token rotation via the admin portal or REST API with a 4-hour grace period... ▸
- \+ Adds an upgrade path from legacy multi-owner tokens to single-owner tokens on a... ▸
- \+ Adds REST API endpoints to create (... ▸

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

BeyondTrust

Feedback ⓘ docs update 2026-07-22 DOCS ↗

◆ NEW PAGE docs.beyondtrust.com

BeyondTrust Pathfinder now supports IdP metadata file import for SAML setup with Entra ID, Okta, and PingOne. BeyondTrust Pathfinder adds SAML SSO identity provider support with group claims, default access rules, and IdP-initiated provisioning. BeyondTrust introduces multi-site management for grouping applications by team, region, or org structure.

Read the new page on docs.beyondtrust.com →

└──▷ DETAILED CHANGES · 21

- + Adds IdP metadata file import in Pathfinder to streamline SAML configuration for...
- + Supports domainless IdP configuration in Pathfinder, enabling administrators to test...
- + Automatically sets ACS URL and Service Provider Entity ID to the same value when...
- + Supports connecting any SAML-compatible identity provider (e.g., Entra/Azure, Okta) to...
- + Adds IdP-initiated authentication flow to auto-provision Pathfinder accounts for users...
- + Introduces default access rules to automatically assign roles (Standard User or...
- + Enables SAML group claims passthrough so Pathfinder applications can consume IdP group...
- + Provides UI workflows under Administration > Identity & Authentication Providers to...
- + New Sites feature lets administrators group BeyondTrust applications by company...
- + Supports switching between sites from the top-right site name drop-down on the BeyondTrust Home page.

- Enables renaming a site via Administration > Edit Site without disrupting access.
- Site deletion removes all associated user permissions and configured connectors immediately and irreversibly.
- New Pathfinder platform provides a single pane of glass across all BeyondTrust SaaS products
- Supports shared single sign-on across all BeyondTrust SaaS products via a central...
- Enables multi-site organization so administrators can group SaaS applications into...
- Supports custom CNAME records with your own SSL certificate to replace the default...
- Supports OAuth-based communication between EPM agents and BeyondInsight (starting in...
- Adds OAuth support for EPM for Mac starting in version 25.2, with Activation ID and...
- Adds Installer Activation Keys UI in BeyondInsight (Configuration > Authentication...
- Starting in U-Series Appliance 4.2, EPM Policy Editor and Privilege Management Reporting (PMR) are automatically installed on appliances — no manual installation required.
- Documents a primary/secondary U-Series Appliance deployment model supporting up to...

WAS THIS USEFUL?

Auth0

Feedback ⓘ docs update 2026-07-23 → 2026-07-27 DOCS ↗

◆ NEW PAGE auth0.com

Auth0 launches Metric Streams (Beta) to stream real-time API metrics to Datadog, New Relic, and Splunk via native or OTLP integrations. Auth0 adds Anonymous Sessions beta and self-service SSO third-party access delegation for customer admins.

Read the new page on auth0.com →

└──▷ DETAILED CHANGES · 8

+	New Metric Streams feature streams real-time Auth0 API metrics (request volume, error... ▸
+	Supports native Datadog integration and OpenTelemetry Protocol (OTLP) for New Relic and Splunk.
+	Exposes `auth0.api_request.count` metric with rich tagging ▸
+	Streams can be enabled, disabled, or deleted independently, retaining configuration when disabled.
+	New Anonymous Sessions (beta, paid plans) ▸
+	Anonymous sessions can be linked to authenticated users through pre-registration and... ▸
+	Anonymous session length is now configurable as a tenant-level setting, and anonymous... ▸
+	Self-Service Enterprise Configuration tickets can now delegate third-party application... ▸

WAS THIS USEFUL? 👍 👎

Nudge Security

Feedback ⓘ changelog · Jul 23, 2026

CHANGELOG ↗

+ NEW IN THE DOCS nudgesecurity.com

Nudge Security adds admin audit log export, inherent/residual risk scores, and automatic business criticality tiers for SaaS and AI apps.

Read on nudgesecurity.com →

└──▷ DETAILED CHANGES · 5

- \+ Exports a complete admin activity log as CSV, capturing OAuth revocations, role... ▸
- \+ Introduces inherent and residual risk scores (Low/Medium/High/Critical) for every SaaS and AI vendor, with transparent factor breakdowns covering vendor security posture, internal deployment risk, and compensating controls — now in open beta.
- \+ Continuously recalculates risk scores as conditions change (e.g., new MCP server... ▸
- \+ Automatically assigns business criticality tiers (Low/Medium/High/Critical) to every app based on inferred data types, enabling inventory filtering across 27 distinct data types with no manual research — now in open beta.
- \+ Allows customization of data sensitivity tiers per organization's data governance... ▸

└──▷ BREAKING ON UPGRADE

! Previously tagged data types are no longer in the main Data Types field; they now appear under Data Types (Legacy), separate from the new automatically populated Data Types field.

WAS THIS USEFUL? 👍 👎

iDenfy

Feedback ⓘ changelog · Jul 24, 2026

SEEN 2026-07-23 → 2026-07-24 CHANGELOG ↗

+ NEW IN THE DOCS documentation.idenfy.com

iDenfy Risk Assessment now integrates with KYB (Know Your Business) workflows. iDenfy dashboard adds PDF generation, blocklist setup, bank card verification, and new workflow steps. iDenfy adds Bank Card Verification, Face Authentication in Dashboard, questionnaires, and expanded KYB/AML features.

Read on documentation.idenfy.com →

└──▷ DETAILED CHANGES · 41

⇄ Full diff

- \+ Supports shared identity verification across companies in KYB (Know Your Business) workflows.
- \+ Adds KYB with Risk Assessment integration, enabling business entity risk reviews...
- \+ Adds PDF Generation configuration option in dashboard setup.
- \+ Adds Blocklist Setup for managing blocklisted identities via the dashboard.
- \+ Adds Sole Proprietorship Workflow Step for business verification flows.
- \+ Adds Proof of Address and Custom Steps configuration in the dashboard.
- \+ Adds Bank Card Verification as a new verification capability.
- \+ New Bank Card Verification confirms the bank card used during onboarding belongs to the verified user.
- \+ New Face Authentication capability available directly in the Dashboard.
- \+ Supports setting up Questionnaires for both KYC and KYB workflows.
- \+ New KYC Data Retrieval feature documented.
- \+ Expanded AML Available Sanctions Lists coverage.
- \+ Additional KYB Features added to the platform.

- Adds Bank Card Verification as a supported KYC identity check in the dashboard.
- New Custom Rule Blocklist configuration available in dashboard settings.
- New Email Template Setup for customizing outbound email content.
- New System Notifications supporting both webhooks and email delivery channels.
- Supports eIDAS compliance for identity verification workflows meeting EU electronic identification standards.
- New Zapier Webhooks integration enables no-code automation of iDenfy verification events.
- New Shopify integration allows merchants to embed iDenfy identity verification directly into their store flows.
- Adds Bank Verification capability accessible directly from the Dashboard.
- Introduces Magic Link feature for streamlined user authentication flows in the Dashboard.
- Adds Branding (KYC) configuration, enabling customization of the KYC experience from the Dashboard.
- Supports creating new companies (multi-company management) within the Dashboard.
- Enables Request Update workflows directly from the Dashboard.
- New MCP server at `https://documentation.idenfy.com/mcp` connects AI assistants...
- Exposes `search_idenfy_documentation` tool
- Exposes `get_page_idenfy_documentation` tool
- Covers all iDenfy products
- Enables AI-assisted KYC/KYB integration code generation, webhook debugging, error-code...
- New Bank Card Verification capability for validating payment card ownership during onboarding flows.

+ New KYB shared identity verification allows a verified identity to be reused across multiple companies.

+ New Blocklist API endpoint for programmatically managing blocklisted identities.

+ Supports PNG format for logo uploads.

+ New Bank Card Verification step confirms the card used during onboarding belongs to the...

+ New POST `/kycidentifications/blocklists` API endpoint enables adding entries to the KYC blocklist programmatically.

+ New DELETE `/kycidentifications/blocklists` API endpoint enables removing entries from the KYC blocklist programmatically.

+ New Suspected Status reference documents why a verification resolves to SUSPECTED and...

+ New Status Handling guide maps every iDenfy verification status to recommended actions...

+ New Supported Browsers reference documents which browsers are compatible with iDenfy's...

+ Supports Zapier Webhooks integration, enabling identity verification events to trigger...

WAS THIS USEFUL? 👍 👎

Clerk

Feedback ⓘ changelog · Jul 24, 2026 2026-07-23 → 2026-07-24

CHANGELOG ↗

+ NEW IN THE DOCS clerk.com

Clerk CLI gains a `clerk mcp` command group for one-command MCP server registration across 10 AI clients, plus configurable default OAuth scopes. Clerk launches a remote MCP server giving AI agents like Claude, Cursor, and Copilot access to up-to-date SDK snippets and auth patterns. Clerk CLI gains `clerk mcp` commands to connect AI coding clients to Clerk's MCP server for live SDK snippets.

Read on clerk.com →

└──▷ DETAILED CHANGES · 16

+ Adds `clerk mcp install` command that detects supported AI clients (Claude Code…

+ Adds `--client` and `--all` flags to `clerk mcp install` for non-interactive, scripted…

+ Adds `clerk mcp run`, a built-in stdio↔Streamable-HTTP bridge that replaces the…

+ Adds `clerk mcp list` to display every Clerk MCP entry registered across all clients…

+ Extends `clerk doctor` to probe the configured Clerk MCP server with a real…

+ Supports configuring default OAuth scopes for dynamic client registration via the OAuth…

+ New remote Model Context Protocol (MCP) server at `https://mcp.clerk.com/mcp` lets AI…

+ New `clerk mcp install` CLI command auto-detects and registers the MCP server across…

+ New `clerk mcp list` and `clerk mcp uninstall` commands manage registered MCP entries…

+ Exposes two MCP tools: `clerk_sdk_snippet` for fetching specific code patterns and...

+ Ships pre-built snippet bundles for B2B SaaS with Organizations/Billing, waitlist...

+ New `clerk mcp install` command registers Clerk's MCP server with AI clients detected...

+ New `clerk mcp list` command shows which AI clients have Clerk's MCP server registered.

+ New `clerk mcp uninstall` command removes Clerk's MCP server registration from detected AI clients.

+ MCP install runs non-interactively in agent mode, targets all detected clients by...

+ `clerk doctor` now validates whether the configured Clerk MCP server is reachable as part of its integration checks.

└──▷ **BREAKING ON UPGRADE**

! Beginning January 18, 2027, CBC-mode SSL/TLS cipher suites (including `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA`, `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA`, `TLS_RSA_WITH_AES_256_CBC_SHA`, and others) will be removed from Clerk-managed subdomains (`clerk.example.com`, `accounts.example.com`); clients that can only negotiate a CBC cipher will fail the TLS handshake after their subdomain's certificate rotates.

WAS THIS USEFUL?  

Ping Identity

Feedback ⓘ changelog · Jul 24, 2026

2026-07-23 → 2026-07-24 CHANGELOG ↗

+ NEW IN THE DOCS docs.pingidentity.com

Ping Identity AIC adds email scripting, secrets in nodes, Rich Authorization Requests, SAML metadata import options, and a new validate-secrets endpoint. LDAP gateway 4.4.0 adds group LDAP filter support for selective inbound provisioning to PingOne.

Read on docs.pingidentity.com →

└──▷ DETAILED CHANGES · 18

+ Adds `emailService` binding for next-generation scripts, enabling email delivery directly from journey scripts.

+ New realm-level OAuth2 Provider setting enables Rich Authorization Requests (RFC 9396)... ▸

+ Individual OAuth 2.0 clients can now be configured with `Authorization Detail Type(s)` ... ▸

+ Dynamic client registration requests now support `authorization_details_types` to... ▸

+ SAML metadata import now supports skipping signature verification.

+ Introduces Patch Object node v2.0, which always updates managed identity objects as... ▸

+ OAuth 2.0 request state is now stored in CTS (Core Token Service) instead of an... ▸

+ Custom report parameters can now be marked as optional, providing more flexibility when running reports.

+ Proxy Connect enabled tenants can now manage Proxy Connect configuration directly in... ▸

+ Hosted journey pages now display hCaptcha text and challenges in the end user's configured locale.

+ Column visibility preferences for data tables in the admin console and hosted account... ▸

+ Super administrators can now configure the redirect URI to use a custom domain when...

+ Social identity providers can now be created and edited directly in the Advanced Identity Cloud admin console.

+ Self-service journey mappings can now be configured directly in the Advanced Identity Cloud admin console.

+ The promotions API now returns report metadata ordered by creation date, most recent first.

+ Journey annotation notes now display multi-line formatting in view mode.

+ Page node v3 is now available, generating a new CAPTCHA token for each validation...

+ Supports group LDAP filters for inbound provisioning, enabling selective sync of LDAP...

WAS THIS USEFUL?  

Didit

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.didit.me

Didit adds phone and email OTP verification APIs with intelligence reporting, risk actions, and sandbox support

Read on docs.didit.me →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- \+ New `POST /v3/phone/verify/` endpoint verifies OTPs and returns phone intelligence ▸
- \+ New `POST /v3/email/verify/` endpoint verifies OTPs and returns email intelligence ▸
- \+ Configurable risk actions (`duplicated_phone_number_action` ... ▸
- \+ 3-attempt budget enforced on both phone and email OTP checks ▸
- \+ Sandbox mode for both verify endpoints ▸
- \+ Finalized OTP checks persist to the originating session (visible in Business Console... ▸
- \+ Backend-only resubmit throttle ▸

WAS THIS USEFUL? 👍 👎

ConductorOne

Feedback ⓘ docs update 2026-07-24 → 2026-07-28

DOCS ↗

+ NEW IN THE DOCS c1.ai

ConductorOne MCP server registration gains discovery-issue acknowledgment flow, custom tool prefix override, and per-server tool enablement control. ConductorOne AI Assistant gains visual report generation with charts, stat cards, tables, and full data lineage verification. ConductorOne adds AI-driven workflow approvals, per-user connector auth, custom campaign recurrence, and richer AI reporting.

Read on c1.ai →

└──▷ DETAILED CHANGES · 49

⇄ Full diff

- + Adds a pre-registration discovery check that surfaces relaxable authorization server...
- + Supports an optional tool prefix override on MCP server registration; falls back to the...
- + Adds per-server tool enablement setting (Require enablement or Auto-enable) that...
- + Generates visual reports with charts, stat cards, and tables directly in the AI Assistant response — no file download required.
- + Supports side-by-side multi-chart dashboards in a single query (e.g., trend chart...
- + Composes full reports combining aggregate stat cards, trend charts, and data tables in one response.
- + Adds a View lineage Data lineage drawer showing the exact query and row count behind...
- + Enables copying individual source queries or the entire lineage (sources, verification...
- + Assigns a workflow step in a request or review policy to C1 AI, which evaluates each...

+ Adds an indirect-access section to entitlement search results, surfacing entitlements...

+ Enables custom recurrence intervals on campaign templates (e.g., every two days, every...

+ Adds a button to open raw access-review and task-detail data as a readable, collapsible...

+ Supports adding groups to a request catalog or access profile so users can request...

+ Holds provisioning requests for entitlements not yet recognized by C1 (e.g., created...

+ Supports combined step-up (MFA) authentication and comment requirements on a single...

+ Adds a View lineage action on C1 AI-generated reports to inspect the exact queries...

+ Renders multiple C1 AI-requested charts as an aligned grid with individual export and source links; C1 AI can also respond with a composed report combining stat cards, a trend chart, and a data table — each with sourcing.

+ Allows admins to require per-user connector credentials (OAuth2, bearer token, custom...

+ Adds automated scheduling for campaign templates, enabling draft campaign instances to...

+ Supports configurable recurrence intervals (e.g., every 2 days, every 3 months) and...

+ New read-only AI > Conversations page lets admins review AI agent conversations across...

+ New System tab surfaces agent policy step evaluations

+ Adds Retry failed provisioning action to re-attempt a failed connector provisioning...

+ Supports bulk retry of multiple failed provisioning tasks via the bulk actions menu.

+ Adds a View policy button in the resource details drawer that opens attached policy...

+ Assign an AI Agent step to any request or review policy workflow, configuring agent...

+ Catalog search now returns an `Entitlements matching` section showing entitlements that...

+ Access review campaigns can now review grants held by groups or roles (not just users)...

+ Campaign templates support custom recurrence intervals (e.g., every 2 days or every 3...

+ IAM policy documents on AWS resources now render as a readable, collapsible JSON tree...

+ Requests for entitlements created ahead of a connector sync (e.g., via Terraform) now...

+ C1 groups can now be added to a request catalog or access profile, making group...

+ Failed connector provisioning on an access task can now be retried directly via 'Retry...

+ Step-up (MFA) approvals that also require a comment can now be completed together in a single flow.

+ External MCP servers now support per-user authentication (OAuth2, bearer token, custom...

+ AI-generated reports include a `Data lineage` view showing the exact queries behind...

+ Ask C1 AI now renders multiple requested charts as an aligned grid and can produce...

+ The CEL editor gains a `Generate` action that converts a plain-English description...

+ Tool enablement (require enablement vs. auto-enable) can now be set per MCP server...

+ External and hosted MCP servers that fail relaxable OAuth discovery checks (e.g....

+ Hosted MCP servers now default to using the tool prefix declared by the connector...

+ Any user can now use the Limit Scopes selector when creating a personal API key to...

+ Adds a Grant type attribute to campaigns and campaign templates, enabling access...

+ Adds JWT Bearer (RFC 7523) authentication support for MCP server connections.

+ Supports MCP (Model Context Protocol) clients for AI access management integration.

+ Adds admin controls to disable MCP traffic.

+ Adds admin controls to disable system features.

+ Enables interaction with the C1 AI assistant directly via Slack DMs once the C1 app for Slack is installed.

+ Documents the C1 MCP integration as a programmatic path for external AI clients (such...

WAS THIS USEFUL? 👍 👎

Omada Identity

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS documentation.omadaidentity.com

Omada Identity Cloud Application Gateway now supports deployment on Linux in addition to Windows.

Read on documentation.omadaidentity.com →

└──▷ WHAT'S NEW IN THE DOCS ▸

WAS THIS USEFUL? 👍 👎

JumpCloud

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS jumpcloud.com

JumpCloud adds an Admin Portal Homepage with organization health alerts and quick admin tasks.

Read on jumpcloud.com →

└──▷ WHAT'S NEW IN THE DOCS ▸

WAS THIS USEFUL? 👍 👎

Okta Identity Engine

Feedback ⓘ docs update 2026-07-27

DOCS ↗

+ NEW IN THE DOCS developer.okta.com

Okta Open Source MCP Server GA: AI agents can now manage identity, brands, and device policies via natural language with least-privilege OAuth scoping. Okta adds OIN Wizard support for Identity Verification integrations and an open-source MCP server for AI agent access to Okta APIs.

Read on developer.okta.com →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- \+ Introduces the Okta Open Source Model Context Protocol (MCP) Server, a secure...
- \+ Adds customization tools for AI clients to manage Okta brands, custom domains, sign-in...
- \+ Adds scope-based tool loading that exposes only the tools permitted by the...
- \+ Adds Device Assurance Policy tools enabling AI agents to programmatically retrieve...
- \+ Integrates the MCP Elicitation API to require explicit human confirmation before...
- \+ ISVs can now build, test, and submit Identity Verification (IDV) integrations to the...
- \+ New open-source Okta MCP Server acts as a secure protocol abstraction layer enabling AI...

WAS THIS USEFUL? 👍 👎

BUILD

◆ AI Coding Agents

Pi

Feedback ⓘ docs update 2026-07-22 → 2026-07-25 DOCS ↗

◆ NEW PAGE pi.dev

Pi 0.80.6 adds a new `max` thinking level above `xhigh` and request-wide input-token pricing tiers for long-context cost accounting. Pi 0.80.7 adds cache-friendly dynamic tool loading, Ctrl+X message copy, Fable 5 extended thinking levels, and toolChoice support for OpenAI/Codex Responses. Pi 0.80.8 adds unified ModelRuntime, live model catalog refresh, xAI device-code OAuth, and Grok 4.5 Responses support.

Read the new page on pi.dev →

└──▷ DETAILED CHANGES · 56

- + Adds `max` thinking level opt-in above `xhigh`, natively supported on GPT-5.6 and...
- + Adds request-wide input-token pricing tiers for accurate long-context cost accounting...
- + Adds `~` (home directory) expansion support for the `shellPath` setting.
- + Adds cache-friendly dynamic tool loading
- + New Ctrl+X shortcut copies the last assistant message, or the selected message in...
- + Adds native xhigh and max thinking levels for Claude Fable 5 across all generated provider catalogs.
- + Adds toolChoice support for OpenAI and Codex Responses providers, including required and named tool selection.
- + Introduces `ModelRuntime` as the canonical async SDK facade, centralizing model...
- + Adds provider-owned `/login` discovery directly from registered pi-ai providers...
- + Adds `pi update --models` command to force an immediate model catalog refresh without updating pi or extensions.

- Adds live background refresh in `/model`
- Adds file-backed dynamic catalogs in `models-store.json`, per-provider pi.dev catalog...
- Adds extension provider refreshModels(context) support for dynamic model discovery with...
- Adds xAI device-code OAuth login so users can sign in to xAI interactively.
- Adds Grok 4.5 OpenAI Responses API support with low, medium, and high thinking levels.
- Adds Kimi K3 model support across built-in providers including Kimi Coding, Moonshot...
- Adds Kimi deferred tool loading for extension-driven progressive tool activation via Kimi's native protocol.
- Changes the default xAI model to Grok 4.5 and updates xAI login to use a prefilled...
- Adds built-in llama.cpp router support with `/login` connection setup and `/llama` ...
- Enables extensions to register complete pi-ai providers with native authentication...
- Adds Qwen Token Plan and Qwen Token Plan China as built-in providers with regional endpoints and API-key authentication.
- Expands usage accounting to persist tool, compaction, and branch-summary usage in...
- Adds `get_available_thinking_levels` RPC command and...
- Exports message and tool execution lifecycle event types from the package root.
- Adds Claude Opus 5 support on Anthropic and Amazon Bedrock with adaptive thinking...
- New `ANTHROPIC_AUTH_TOKEN` environment variable authenticates against Anthropic-compatible gateways requiring
- Pi.dev model catalogs now revalidate using `If-None-Match`, so unchanged providers...

+ Exposes the `outputPad` setting to custom message renderers via the Extensions API.

+ Adds `/login` OAuth flow for OpenRouter (PKCE) and Kimi Code subscriptions, eliminating manual API key configuration.

+ Exposes `PI_SESSION_ID`, `PI_SESSION_FILE`, `PI_PROVIDER`, `PI_MODEL`, and...

+ Adds `PI_CODING_AGENT_DIR` and `PI_CODING_AGENT_SESSION_DIR` to override config and session storage directories.

+ Adds `PI_CACHE_RETENTION=long` to enable extended provider prompt caching where supported.

+ Adds `PI_OFFLINE` to disable all startup network operations including update checks and telemetry.

+ Adds `PI_TELEMETRY` to override install/update telemetry and provider attribution headers.

+ Adds `PI_HARDWARE_CURSOR=1` to enable hardware cursor display.

+ Adds `PI_SHARE_VIEWER_URL` to override the base URL used by `/share`.

+ Supports `HTTP_PROXY` / `HTTPS_PROXY` for proxying outbound HTTP requests.

+ Radius OAuth device authorization, token exchange, and refresh requests now route...

+ Model loading errors now append the underlying cause (e.g. provider OAuth failure) for clearer diagnostics.

+ Adds `ctx.modelRegistry`, `ctx.model`, and `ctx.thinkingLevel` to expose the active...

+ Injects session environment variables (`PI_SESSION_ID`, `PI_SESSION_FILE`...

+ Adds

+ Adds `Tool.constrainedSampling` to let tools prefer or require strict JSON Schema...

+ Adds `supportsGrammarTools`, `supportsStrictTools`, and expanded `supportsStrictMode`...

- Adds OAuth PKCE sign-in for OpenRouter, minting a user-controlled API key without manual configuration.
- Adds inherited Kimi Code subscription OAuth login for the Kimi For Coding provider...
- Exposes `PI_SESSION_ID`, `PI_SESSION_FILE`, `PI_PROVIDER`, `PI_MODEL`, and...
- Adds streaming `bash_execution_update` events for direct RPC bash commands, correlated with request IDs.
- Model catalogs now expose only provider-verified reasoning effort levels sourced from models.dev.
- New `summarization_retry_scheduled`, `summarization_retry_attempt_start`, and...
- Adds OpenRouter as a sign-in provider via PKCE OAuth flow, creating a user-controlled...
- Adds Google Gemini 3.5 Flash Lite (`google/gemini-3.5-flash-lite`) as a new available model.
- Adds Google Gemini 3.6 Flash (`google/gemini-3.6-flash`) as a new available model.
- Adds Poolside Laguna S 2.1 (`poolside/laguna-s-2.1`) and a free tier variant...
- Adds deterministic, checksummed source archives to GitHub releases with documented...
- Transient provider failures during compaction and branch summaries now follow the...

WAS THIS USEFUL?

Goose

Feedback ⓘ docs update DOCS ↗

◆ NEW PAGE goose-docs.ai

Goose adds rp-why skill: an AI collaboration coach that scores your tool sophistication and prompt depth.

Read the new page on goose-docs.ai →

└──▷ DETAILED CHANGES · 5

+	New `rp-why` skill analyzes conversation history to score sessions on Gas Town Stage...
+	New `/rp-why init` command establishes a personal baseline by analyzing available conversation history (~30 seconds).
+	New `/rp-why current` command shows how the active session compares to your typical usage patterns.
+	New `/rp-why compare` command diffs the current session against your baseline to surface progress or regression.
+	Session output includes a quadrant map (Underutilizing / Frontier / Learning Zone /...

WAS THIS USEFUL? 👍 👎

OpenHands

Feedback ⓘ docs update 2026-07-28 DOCS ↗

◆ NEW PAGE docs.openhands.dev

OpenHands Agent Canvas adds a prebuilt GitHub PR Review workflow that watches pull requests and posts automated reviews. OpenHands adds Agent Canvas UI, persistent memory, path-triggered rules, SDK plugins, and full Kubernetes/Enterprise deployment docs.

Read the new page on docs.openhands.dev →

└──▷ DETAILED CHANGES · 13

- \+ New prebuilt GitHub PR Review workflow in Agent Canvas lets an OpenHands agent...
- \+ GitHub MCP Server integration in Agent Canvas provides the agent tools for reading...
- \+ Configurable review scope lets the automation target specific repositories, post single...
- \+ New Agent Canvas: a desktop UI for running agents with reusable profiles, conversation...
- \+ Adds opt-in two-tier persistent memory that survives across conversations via the SDK.
- \+ Introduces path-triggered rules that deterministically inject context whenever an agent...
- \+ Supports plugin discovery, installation, and attachment directly inside Agent Canvas.
- \+ Enables custom sandbox images so agents start with pre-loaded repos, dependencies, and tooling.
- \+ Adds Docker-in-sandbox capability, letting agents run containers, Docker Compose, and...
- \+ New Azure DevOps integration for authentication and automation triggers in OpenHands Enterprise.
- \+ Adds Laminar-based analytics for trace analysis in OpenHands Enterprise.

+ Supports mobile access to Agent Canvas via Tailscale or ngrok.

+ Enterprise Skills and Plugins management for repository, organization, and user-scoped skills.

WAS THIS USEFUL? 👍 👎

Cline

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.cline.bot

Cline adds Hooks support plus two new AI providers: MiniMax and Poolside.

Read on docs.cline.bot →

└──▷ DETAILED CHANGES · 3

⇄ Full diff

+ Adds Hooks integration for extending Cline via SDK plugins.

+ Adds MiniMax as a supported AI provider for model configuration.

+ Adds Poolside as a supported AI provider for model configuration.

WAS THIS USEFUL? 👍 👎

PLATFORMS & UTILITIES

◆ General Utilities & Libraries

Microsoft code-oss

Feedback ⓘ docs update 2026-07-23

DOCS ↗

+ NEW IN THE DOCS code.visualstudio.com

VS Code enterprise policies gain MCP server allowlist/denylist controls and Copilot Chat OpenTelemetry export settings. VS Code 1.130: agent sessions in dedicated processes, assisted tool approvals, multi-file diff review, and Git diff file opening.

Read on code.visualstudio.com →

└──▷ DETAILED CHANGES · 7

⇄ Full diff

- \+ Adds `ChatAllowedMcpServers` policy to allowlist which Model Context Protocol servers can be installed or run.
- \+ Adds `ChatDeniedMcpServers` policy to denylist MCP servers that must be blocked, with... ▸
- \+ Adds OpenTelemetry export configuration policies for Copilot Chat, including... ▸
- \+ Runs agent sessions in a dedicated process for improved isolation and stability.
- \+ Reduces approval interruptions with assisted tool approvals in agent workflows.
- \+ Enables faster multi-file change review directly in the Agents window.
- \+ Supports opening files directly from Git diffs in the terminal.

.

WAS THIS USEFUL? 👍 👎

kubernetes-helm

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS helm.sh

Helm now supports `SOURCE_DATE_EPOCH` for reproducible chart archives across builds and machines.

Read on helm.sh →

└─▷ DETAILED CHANGES · 3

⇄ Full diff

- \+ Supports the `SOURCE_DATE_EPOCH` environment variable to produce byte-identical chart... ▸
- \+ Stamps the `generated:` timestamp in Chart.lock with `SOURCE_DATE_EPOCH`, making... ▸
- \+ Extends `SOURCE_DATE_EPOCH` support to `helm install`, `helm dependency build`, and... ▸

WAS THIS USEFUL? 👍 👎

curl

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS curl.se

curl 8.22.0 extends `--xattr` Windows support, writing Zone.Identifier Alternate Data Streams with HostUrl and ReferrerUrl.

Read on curl.se →

└─▷ WHAT'S NEW IN THE DOCS ▸

WAS THIS USEFUL? 👍 👎

OpenSSL

Feedback ⓘ docs update DOCS ↗

+ NEW IN THE DOCS docs.openssl.org

OpenSSL adds three new `ASN1_STRING` API functions for length and data manipulation.

Read on docs.openssl.org →

└──▷ WHAT'S NEW IN THE DOCS ▸

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · July 29, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue