THE CYBER TOOLCHAIN

NO. 075

Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED SEPTEMBER 15, 2026 · EVERY DAY

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

▸ // HOW THIS ISSUE IS MADE SHOW

VIEW

ISSUE VIEW

scroll



SCROLL | EXPAND IN PLACE | PREVIEW PANE

INFORMATION DENSITY

everything



BRIEFED | EVERYTHING

Every tool in the issue, in full.

all 153 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 30 tools

▾ // THE BRIEF HIDE

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

Three unrelated things stand out. Zeek 9.0 can now ingest mirrored VXLAN/GENEVE traffic directly, so cloud-overlay taps land in your ors without a decap appliance. ZeroPath put a 0–100 score on

vim ? help

findings and moved repo permissions server-side. And InsightIDR can pull Domain Controller security logs through the Insight Agent and act on AD accounts from the console.

DETECT

Get cloud-overlay and Domain Controller traffic into your sensors without extra plumbing

Zeek 9.0's UDP packet source reads VXLAN/GENEVE mirror sessions straight off the wire, removing the decapsulation hop that cloud traffic mirroring normally forces, and adds NTP and multicast logs plus deeper TLS, DCE-RPC, Kerberos and LDAP events. InsightIDR collects DC security logs via the Insight Agent, so the usual WEF/collector chain for the noisiest and most valuable log source on the estate goes away.

Zeek · InsightIDR

PROTECT

Triage application findings by rank instead of by severity bucket

ZeroPath's 0–100 priority score plus refined CVSS and SCA severity handling gives an ordered queue rather than a pile of Highs, and repository permissions are now enforced server-side rather than in the UI. Codex Security's `$codex-security:assess-patch-risk` and `$codex-security:verify-fix` close the other end — judging whether a proposed fix actually lands before it ships.

ZeroPath · OpenAI Codex Security

RESPOND

Contain a compromised AD account from the same console you saw the alert in

InsightIDR's Active Directory response actions cut the hop to a domain admin console during the first minutes of an account-takeover investigation. Threat Command adds an IOC enrichment pivot from Rapid7 SIEM and Automation into the Threat Intelligence database, plus a query language for alert search, so checking whether an indicator is already known stops being a copy-paste into a second tab.

InsightIDR · Threat Command

OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

sippts

Feedback ⓘ 1 RELEASE · 2026-09-14 NOTES ↗ RANK

Set of tools to audit SIP based VoIP Systems

> sippts v4.2.1 adds CVSS-based severity scoring to CVE detection results, sorting findings from most to least severe.

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

01 **CVSS scoring for CVE results** IMPROVED 65

The scan module now assigns CVSS scores with severity colours to detected CVEs and orders findings worst-first. This is backed by a 6th column added to `data/cve.csv` carrying the CVSS score (list version 0.5), which requires sippts 4.2.1 or newer to read.

— Names exact file, column addition, and version requirement. v4.2.1

WAS THIS USEFUL? 👍 👎

SensePost gowitness

Feedback ⓘ 1 RELEASE · 2026-09-14

NOTES ↗ RANK

gowitness - a golang, web screenshot utility using Chrome Headless

> gowitness 3.2.0 adds support for reusing authenticated Chrome sessions during scans and a flag to disable colored log output.

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

01 Reuse authenticated Chrome sessions via user data dir NEW

77

The new `--chrome-user-data-dir` flag lets you point gowitness at an existing Chrome User Directory, enabling reuse of an already-authenticated browser session (e.g. after manually logging into an SSO portal) across gowitness runs instead of re-authenticating each scan.

Screenshot targets while inheriting an already-authenticated Chrome profile (e.g. after manually logging into an SSO portal) to avoid re-authenticating during a scan.

```
$ gowitness scan single --url "https://internal.corp.example.com"
--write-db --chrome-user-data-dir ~/.config/google-chrome/Default
```

— Named flag with clear mechanism and runnable example command. 3.2.0

THINNER COVERAGE BELOW

02 Disable ANSI color in log output NEW

45

A new `--no-log-color` global flag disables ANSI color codes in gowitness's log output.

— Named flag but no example or further context given. 3.2.0

WAS THIS USEFUL? 👍 👎

APPLICATION SECURITY

◆ SAST / SCA / Code Security

GitHub

Feedback ⓘ 1 RELEASE · 2026-09-14 BLOG ↗ RANK

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

> GitHub Copilot's auto model selection now lets users tune the cost-quality tradeoff with new optimization tiers, rolled out across VS Code, Copilot CLI, and the GitHub Copilot app.

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

01 **Configurable tiers for Copilot auto model selection** NEW

65

Copilot auto model selection gains three optimization tiers — `efficiency`, `balance`, and `intelligence` — letting users control how auto weighs cost, quality, and response latency per prompt. The tier configuration is rolled out in Visual Studio Code, Copilot CLI, and the GitHub Copilot app.

— Names tiers and surfaces but no config steps or defaults

Configure cost and quality in Copilot a…

WAS THIS USEFUL? 👍 👎

Cloudsmith

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

A fully-managed, enterprise-scale solution to control, secure, and distribute software packages and containers.

> Cloudsmith's latest release focuses on visibility and access control: teams can now export vulnerability findings, audit per-package changes, grant narrower read-only roles, and get richer GitHub secret-scanning alerts.

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

01 Granular billing, usage and OIDC read-only roles NEW

60

Workspace owners can now grant members individual read-only access to billing, usage, and OIDC data without assigning the Manager or Owner role, via separate toggles for Billing, Usage, and OIDC privileges under Workspace Settings > Members.

Give a finance or compliance team member visibility into billing and OIDC configuration without elevating their role to Manager or Owner.

> 📍 In the Cloudsmith web app, go to Workspace Settings › Members, select the member, and enable the individual Billing, Usage, or OIDC read-only privilege toggles separately.

— Names exact toggles and settings path, no API surface given.

changelog-20260915-48925691

THINNER COVERAGE BELOW

02 Richer GitHub secret-scanning alert emails IMPROVED

40

GitHub secret-scanning email notifications now list every location an exposed Cloudsmith API key was found in a GitHub repository, each with a direct link to the detection.

— Describes the improvement but gives no actionable config or command.

changelog-20260915-48925691

WAS THIS USEFUL? 👍 👎

◆ Web Application Security

Invicti

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

Official documentation for Invicti AppSec Platform, Invicti Platform, and Invicti Enterprise — web application security testing, DAST, API security, and vulnerability management.

> Invicti's scan location exports now surface HTTP method and status code data across CSV, JSON, and XML formats, making it easier to spot authentication gaps in crawl coverage.

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

01 **HTTP method and status code columns in scan location exports**

IMPROVED 70

Scan location exports now include HTTP Methods and Status Codes fields. The CSV (Locations) export gets these columns appended at the end of each row, and the JSON and XML scan location export formats gain matching HTTP method and HTTP response code fields.

After a scan completes, export locations in CSV to spot routes returning 401 or 403 — indicating authentication gaps in crawl coverage.

> 📍 In the scan results, go to Scan › Locations › Export, select CSV (Locations), then open the file and filter the Status Codes column for 401 or 403 responses.

— Names exact formats and fields, plus a concrete usage path. changelog-20260915-35c4580b

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Levo

Feedback

2 RELEASES · 2026-09-08 → 2026-09-15

NOTES ↗

RANK

Continuous API Security Assurance â observe, detect, and protect your APIs.

> Levo shipped a synchronous CreateFinding API mode, per-application security-test configuration overrides, a beta Service Graph for visualizing API call relationships, expanded RBAC permissions and audit logging, broader form-encoded body and unauthenticated-access testing, plus a new API discovery source and two new integrations.

└──▷ **WHAT SHIPPED · 11 FEATURES** most completely described first ? what's the number?

01 **RBAC permissions and audit logging expansion** NEW 80

Adds Test Runs update and delete permissions, with Owner and Admin holding them by default while other roles require explicit grants; adds Admin-wide delete permissions across the platform; grants Security Engineer the ability to delete endpoints; and adds role and permission changes to the audit log under a new Role resource type, recording the role's identifier, permission set, and user-assignment actions as distinct events.

— Names permissions, defaults, and new audit resource type in detail.

SaaS Platform Services -- 1.2.135.1

02 **Per-application security-test configuration overrides** NEW 75

Adds per-application security-test configuration overrides via a new Configuration tab on each application's Security Testing page, with settings marked as inherited from the environment or overridden for that application.

Override rate-limit and other security-test settings for a single high-traffic application without affecting environment-wide defaults.

📍 In the Levo console, open the application, go to Security Testing › Configuration tab, locate the setting you want to change (e.g., rate limit), toggle it from Inherited to Override, and set the desired value (shown in requests per minute).

— Exact UI path and worked example of overriding a setting.

SaaS Platform Services -- 1.2.135.1

03 **Service Graph (Beta) in API catalog** NEW 70

Adds Service Graph (Beta) to the API catalog, visualizing call relationships between services; enabled per workspace from admin settings.

Enable the Service Graph (Beta) for a workspace so your team can visualize which services call one another across your API catalog.

📍 In the Levo console, go to Admin Settings › Workspace, find the Service Graph (Beta) toggle, and enable it for the target workspace.

— Exact enablement navigation given in example. SaaS Platform Services -- 1.2.135.1

04 **Synchronous CreateFinding API mode** NEW 65

Adds `CreateFinding` API opt-in synchronous mode that returns event IDs on completion; default asynchronous behavior is unchanged.

— Names the API and behavior change but no request example.

SaaS Platform Services -- 1.2.135.1

05 **On-Prem Deployments monitoring and setup** NEW 60

Adds an `Active / Stale / Down` status filter on the On-Prem Deployments screen for Satellites, Taggers, Sensors, DAST Runners, and AI Gateways alongside the existing lifecycle filter, and adds an Install Satellite action to the Taggers tab on On-Prem Deployments.

— Names filter values and new action but no example. SaaS Platform Services -- 1.2.135.1

06 **Unauthenticated-access probing in Broken User Authentication tests**

IMPROVED 60

Extends Broken User Authentication tests to probe for unauthenticated access even when no authenticated baseline is available, reporting genuine resource-shaped responses as Medium, low-confidence unconfirmed findings.

— Explains mechanism and severity labeling, no config surface.

SaaS Platform Services -- 1.2.135.1

THINNER COVERAGE BELOW

07 **Bulk delete for API scans** NEW 55

Adds bulk delete for API scans from the API Scans list, governed by the Test Runs delete permission in workspaces with roles enabled.

— Names the permission gating the action, no example. SaaS Platform Services -- 1.2.135.1

08 **Consolidated component-health alert emails** IMPROVED 50

Consolidates component-health alerts for large fleets into a single email with a CSV listing components oldest-heartbeat first, instead of one email per detection wave.

— Explains the new email format and ordering, no config key.

SaaS Platform Services -- 1.2.135.1

09 **Form-encoded body testing** NEW 45

Extends API security testing to form-encoded request bodies, so URL-encoded form parameters are correlated and tested like any other structured body.

— Describes scope of coverage but no setup detail. SaaS Platform Services -- 1.2.135.1

10 **New API discovery source** NEW 15

Adds a new API discovery source for broader API inventory coverage.

— No details on which source or how to enable it. Release Notes — September 1–8, 2026

11 **Two new integrations** NEW 5

Introduces two new integrations.

— No names or setup details for the integrations given.

Release Notes — September 1–8, 2026

WAS THIS USEFUL?  

◆ Secrets Detection & Management

GitGuardian Detection Engine

Feedback ⓘ

1 RELEASE · 2026-09-15 | CHANGELOG ↗ | RANK

GitGuardian Detection Engine scans code repositories to identify and alert on exposed secrets, credentials, and sensitive data.

> GitGuardian's Detection Engine adds two new secret analyzers, sharpens entropy-based false positive filtering, and improves detection recall for n8n and HashiCorp Vault credentials.

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

01 **Entropy secret filter for checksum variables** IMPROVED

60

Adds a `generic_high_entropy_secret` filter that suppresses false positives when the assigned variable name ends with `checksum`, with no loss of recall.

– Names exact filter and trigger condition, no UI/config path changelog-20260915-84cb4e9d

02 **n8n host detection for MCP and API tokens** IMPROVED

60

Extends the `n8n MCP Access Token` and n8n API Key detectors to recognize n8n hosts given as a container service name or as a scheme-less hostname, and to reject unreachable private IP hosts.

– Names both detectors and exact new host-matching behavior changelog-20260915-84cb4e9d

THINNER COVERAGE BELOW

03 **New analyzers for Akamai and Docker Hub secrets** NEW

45

Adds a secret analyzer for Akamai API Credentials and a new analyzer for Docker Hub personal access tokens.

– Names two new analyzers, no scan mechanism detail changelog-20260915-84cb4e9d

04 **Improved Vault AppRole credential recall** IMPROVED 25

Improves recall for HashiCorp Vault AppRole Authentication credentials.

– Bare improvement claim with no mechanism or scope changelog-20260915-84cb4e9d

WAS THIS USEFUL? 👍 👎

REVERSE ENGINEERING, MALWARE & FORENSICS

◆ Digital Forensics & Incident Response

iLEAPP

Feedback ⓘ 1 RELEASE · 2026-09-14 NOTES ↗ CODE ↗ RANK

iOS Logs, Events, And Plist Parser

> iLEAPP v2026.4.1 upgrades its Apple Unified Logs parser and extends OS version recognition to cover the newest iOS, macOS, tvOS, visionOS, and watchOS releases.

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

01 **Unified Logs engine upgraded to v0.7.0** IMPROVED 57

The Apple Unified Logs parsing engine is upgraded to `unifiedlog_iterator` v0.7.0, which fills previously empty process paths on Simpledump and Statedump rows and logs the parser version at import time.

— Names mechanism and affected row types but no reproduction steps. v2026.4.1

02 **New OS build recognition in build ID map** NEW 45

`apple_build_id_to_os_version.json` gains recognition for iOS 26.7, iOS 27.0, macOS 15.8, macOS 26.7, macOS 27.0, tvOS 27.0, visionOS 27.0, and watchOS 27.0.

— Lists exact versions and file but no behavioral detail. v2026.4.1

WAS THIS USEFUL? 👍 👎

◆ Malware Analysis

Joe Security (Joe Sandbox)

Feedback ⓘ

1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

Automated Malware Analysis - Development and Licensing of Automated Malware Analysis Tools to Fight Malware

> Joe Security shipped Joe Reverser 2.1 Golden Eagle, expanding its agentic automated analyst for malware, phishing, malicious documents and web-based threats, with tighter integration into automated analysis workflows.

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

01 **Joe Reverser 2.1 'Golden Eagle' agentic analyst** IMPROVED

40

Joe Reverser 2.1, codenamed Golden Eagle, is an agentic automated analyst that covers malware, phishing campaigns, malicious documents, and web-based threats, with enhanced autonomous analysis and reverse engineering capabilities. The release also improves integration of Joe Reverser's agentic capabilities into automated analysis workflows.

— Names version and threat categories but no concrete mechanism or interface.

changelog-20260915-5d7810df

└──▷ ALSO FROM THESE RELEASES

WAS THIS USEFUL? 👍 👎

NETWORK SECURITY

◆ Network Analysis & Monitoring

Zeek

Feedback ⓘ 1 RELEASE · 2026-08-21 NOTES ↗ CODE ↗ RANK

Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.

> Zeek 9.0 adds a UDP packet source for VXLAN/GENEVE mirroring, a Spicy-based ZIP file analyzer, new NTP and multicast logs, and expanded TLS, DCE-RPC, Kerberos and LDAP event coverage, while removing Broker's legacy embedded WebSocket server in favor of Cluster::listen_websocket().

└──▷ WHAT SHIPPED · 24 FEATURES most completely described first ? what's the number?

01 **UDP packet source for VXLAN/GENEVE mirroring** NEW 95

Zeek adds a UDP packet source via `zeek -i udp::0.0.0.0:4789:vxlan` (bundled `zeek-packet-source-udp` plugin) to receive VXLAN or GENEVE mirror traffic over UDP without needing raw packet capture, using `SO_REUSEPORT` so multiple workers can kernel-load-balance the traffic. The new `policy/frameworks/conn_key/packet_source/udp/vxlan_vni` policy script adds VNI-aware connection tracking when this source is used.

Receive VXLAN mirror traffic over UDP on a busy sensor where multiple Zeek workers share the load via kernel `SO_REUSEPORT` balancing — no raw packet capture interface needed.

```
$ zeek -i udp::0.0.0.0:4789:vxlan
```

Enable VNI-aware connection tracking so each VXLAN tenant network is tracked separately — load alongside the UDP packet source.

```
$ zeek -i udp::0.0.0.0:4789:vxlan
policy/frameworks/conn_key/packet_source/udp/vxlan_vni
```

— Full command, plugin and mechanism given with runnable examples v9.0.0

02 **Configurable JSON string escape policy** NEW 88

Adds `Log::json_string_escape_policy` (type `JSON::STRING_ESCAPE_POLICY_*`) to make control-character and invalid UTF-8 escaping in JSON logging configurable; default remains `JSON::STRING_ESCAPE_POLICY_HEX`. Setting it to

`JSON::STRING_ESCAPE_POLICY_TSV` in `local.zeek` switches to reversible TSV-style encoding for round-tripping binary fields.

Switch JSON log escaping to TSV-style (reversible) encoding instead of the default hex encoding, so downstream SIEM parsers can round-trip binary fields correctly.

```zeek
redef Log::json_string_escape_policy =
JSON::STRING_ESCAPE_POLICY_TSV;
```

— Exact config key, values, and runnable example given v9.0.0

---

03 **Legacy Broker WebSocket server removed** BREAKING 82

Broker's legacy embedded WebSocket server is fully removed: `Broker::BrokerProtocol`, `Broker::default_port_websocket`, `Broker::default_listen_address_websocket`, `Broker::web_socket_buffer_size`, and `Broker::web_socket_overflow_policy` no longer exist, and the `BrokerProtocol` enum and the Broker manager's Listen() C++ method's optional `BrokerProtocol` argument have been removed. Use Cluster::listen_websocket() and the `ZEEK_WEBSOCKET_*` environment variables instead.

— Names every removed symbol and the migration path v9.0.0

---

04 **Storage framework options for known-* scripts** IMPROVED 80

Extends the `known-certs`, `known-hosts`, and `known-services` scripts with storage-framework options including `enable_hosts_persistence`, `host_store_prefix`, `host_store_backend_type`, and `host_store_backend_options`, using a SQLite backend under `Cluster::default_store_dir` by default.

— Names every option and default backend location v9.0.0

---

05 **zeek::fmt() no longer safe off the main thread** BREAKING 76

Calling zeek::fmt() from non-main threads now emits a warning (and aborts in debug builds); plugins spawning threads must switch to threading::BasicThread::Fmt() or std::format().

— Names replacement APIs and build-mode behaviour v9.0.0

---

06 **Spicy-based ZIP file analyzer** NEW 75

Adds `policy/files/zip/register.zeek` to map the bundled Spicy ZIP file analyzer to the `application/zip` MIME type; recursive ZIP depth is controlled by `Spicy::max_file_depth`.

— Names config script and depth control, no usage example v9.0.0

07 **LDAP SASL payload forwarding to GSSAPI/NTLM** IMPROVED 74

Extends the LDAP analyzer to forward SASL payloads from `bindRequest` / `bindResponse` to the GSSAPI and NTLM parsers, enriching `ntlm.log` and `kerberos.log`.

— Names mechanism and affected logs v9.0.0

08 **Kerberos AP-REQ tracking improvements** IMPROVED 74

Extends krb_ap_request() event with an `in_kdc_padata` parameter to indicate whether the AP-REQ is embedded in KDC/TGS pre-authentication data, and populates the `service` and `cipher` columns in `kerberos.log` AP entries, which were previously unset.

— Names event parameter and log columns, before/after given v9.0.0

09 **New HTTP header validation weirds** NEW 73

Extends the HTTP analyzer with nine new weirds — `HTTP_bad_chunk_size`, `HTTP_chunked_multi`, `HTTP_content_length_0_and_expect_100_cont`, `HTTP_content_length_leading_zeros`, `HTTP_bad_content_length`, `HTTP_obsolete_line_folding`, `HTTP_content_length_and_chunked`, `HTTP_content_range_and_chunked`, and `HTTP_expect_not_100_continue` — for unusual Content-Length, Transfer-Encoding, and Expect header usage.

— Names all nine weirds verbatim v9.0.0

10 **Reporter::limit_reached_weird BIF for size limits** NEW 70

Adds `Reporter::limit_reached_weird` BIF to report size-limit violations, logging a named weird and appending `X` to the connection `history` field.

— Names BIF and the history field effect v9.0.0

11 **New `?as` operator and expanded `as` casting** IMPROVED 68

Adds `?as` operator to test whether a value can be safely cast to a target type at script level, and extends the `as` casting operator to cover all type conversions previously requiring explicit BiFs such as interval_to_double(), plus additional natural companions.

— Names both operators and an example BiF replaced v9.0.0

12 **DCE-RPC authentication event** NEW 65

Adds dce_rpc_auth() event giving script-level access to the security provider, per-message protection, and authentication context in DCE-RPC PDUs.

— Names event and what data it exposes v9.0.0

13 **Multicast participants log** NEW 63

Adds `policy/protocols/conn/multicast-participants.zeek`, producing a new `multicast_participants.log` with IGMP-derived data about hosts participating in multicast connections.

— Names log and script but no field-level detail v9.0.0

14 **New TLS extension events for ECH and signature algorithms** NEW 60

Adds `ssl_extension_encrypted_client_hello`, an event carrying information about the TLS `encrypted_client_hello` extension, and `ssl_extension_signature_algorithms_cert`, raised for the TLS `signature_algorithms_cert` extension.

— Names both events but no field-level detail v9.0.0

THINNER COVERAGE BELOW

15 **Syslog analyzer TCP support** IMPROVED 59

Extends the Syslog analyzer to support TCP via Octet Counting and Non-Transparent-Framing on port 514/tcp.

— Names framing modes and port, no example v9.0.0

16 **QUIC detection signatures for non-standard ports** NEW 59

Adds DPD signatures for QUIC version 1 and QUIC version 2 to attach the QUIC analyzer on non-port-443 UDP connections when a signature match occurs.

— Names versions and ports affected v9.0.0

17 **Non-final OpaqueType for plugin-defined scripting types** NEW 59

Makes `OpaqueType` non-final and adds hooks for hashing, casting, and default initialization, enabling plugins to introduce new scripting types storable in sets/tables and castable to existing Zeek types (experimental).

— Explains mechanism but marked experimental, no example v9.0.0

18 **Standalone ZeroMQ connection without cluster node events**

IMPROVED

59

Splits `zeromq/main.zeek` options into a separate `zeromq/options.zeek` file to allow standalone Zeek processes to connect to the ZeroMQ layer without participating in cluster node events.

— Names file split and use case v9.0.0

19 **Case-insensitive and single-line pattern modifiers in Input Framework**

IMPROVED

57

Extends the Input Framework to read pattern values with case-insensitive (`/foo/i`) and single-line (`/bar/s`) modifiers.

— Names exact modifier syntax v9.0.0

20 **ZeekJS now requires C++20** BREAKING

56

The ZeekJS plugin now requires `std::format` from C++20, dropping support for older distributions using GCC 12.x such as Debian 12.

— Names dropped platform but no migration steps v9.0.0

21 **NTP control and private mode logs** NEW

55

Adds two new logs, `ntp_control.log` and `ntp_private.log` , covering NTP modes 6 and 7, which were previously unlogged.

— Names logs and modes, no field schema given v9.0.0

22 **Attributes field on script_id records** NEW

47

Adds `$attributes` field to `script_id` records returned by global_ids() BiF, exposing identifier attributes.

— Names field and BiF, no usage detail v9.0.0

23 **Multi-interface support in zeek.conf and systemd generator**

IMPROVED

45

Extends `zeek.conf` and `zeek-systemd-generator` to support multiple interfaces and multi-host deployments.

— Named files but no config keys or example shown v9.0.0

24 FreeBSD moved to community-patch support DEPRECATED

41

FreeBSD is no longer officially supported with CI testing; it moves to the same community-patch model as OpenBSD.

— States change but no timeline or migration v9.0.0

└──▷ BREAKING ON UPGRADE

! Broker's legacy embedded WebSocket server is fully removed: `Broker::BrokerProtocol`, `Broker::default_port_websocket`, `Broker::default_listen_address_websocket`, `Broker::web_socket_buffer_size`, and `Broker::web_socket_overflow_policy` no longer exist. Use Cluster::listen_websocket() and the `ZEEK_WEBSOCKET_*` environment variables instead.

! The `BrokerProtocol` enum has been removed and the Broker manager's Listen() C++ method no longer accepts its optional `BrokerProtocol` argument; it always uses Broker's native protocol.

! Calling zeek::fmt() from non-main threads now emits a warning (and aborts in debug builds); plugins spawning threads must switch to threading::BasicThread::Fmt() or std::format().

! The ZeekJS plugin now requires `std::format` from C++20, dropping support for older distributions using GCC 12.x such as Debian 12.

! FreeBSD is no longer officially supported with CI testing; it moves to the same community-patch model as OpenBSD.

WAS THIS USEFUL? 👍 👎

◆ Firewalls & Network Defense

Fastly

Feedback ⓘ 2 RELEASES · 2026-09-14 BLOG ↗ RANK

Fastly is a content delivery network and edge computing platform that accelerates web content delivery and application performance globally.

> Fastly's CLI gained new logging subcommands for Log Explorer and Insights, while the JavaScript SDK added an async method for cache transaction lookups.

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

01 **Async cache transaction lookup in JS SDK** NEW 60

The Fastly JavaScript SDK 3.46.0 adds a `CoreCache.transactionLookupAsync` method for performing asynchronous cache transaction lookups.

– Names exact method but not usage details JavaScript SDK 3.46.0 (2026-09-14)

THINNER COVERAGE BELOW

02 **Log Explorer and Insights CLI commands** NEW 45

The Fastly CLI adds `logging` subcommands for Log Explorer and Insights.

– Names the subcommand but not specific options CLI v16.1.0 (2026-09-14)

WAS THIS USEFUL? 👍 👎

CLOUD & CONTAINER SECURITY

◆ CNAPP

Rapid7 InsightCloudSec

Feedback ⓘ 1 RELEASE · 2026-09-15

DOCS ↗ BLOG ↗ RANK

Rapid7 InsightCloudSec is a cloud security platform that provides visibility, compliance, and threat detection across multi-cloud environments.

> Rapid7 InsightCloudSec's 26.9.15 release adds new Query Filters and Insights covering Azure Cache for Redis, Cosmos DB, and Database Instances (PostgreSQL, SQL Server, MySQL), backed by expanded harvesters that collect the underlying encryption, authentication, and network-access properties.

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

01 **Azure Cache for Redis security visibility** NEW 80

Adds Cache Instance Encryption Type Query Filter to identify Cache Instances by encryption configuration (Customer-Managed Key vs. Provider-Managed Key), defaulting to Provider-Managed Key detection, and Cache Instance Access Key Authentication Enabled Query Filter to identify Azure Cache for Redis instances where `disableAccessKeyAuthentication` is set to false. Adds Insights Cache Instance Not Using Customer Managed Key and Cache Instance With Access Key Authentication Enabled (aligned with CIS Azure Database Services Benchmark v2.0.0 Control 2.9). Expands the Azure Cache for Redis harvester to collect Customer-Managed Key (CMK) encryption properties from Azure Cache for Redis Enterprise resources.

— Names filters, insights and CIS mapping but no exact UI path or API call

2026-09-15-3c05e607

02 **Azure Cosmos DB Distributed Table coverage** NEW 80

Adds Distributed Table Public Network Access Query Filter to identify Azure Cosmos DB accounts with public network access enabled, and Distributed Table Without Diagnostic Logging Query Filter to identify Cosmos DB accounts missing a specified diagnostic log category, defaulting to `allLogs`. Adds Insights Distributed Table With Public Network Access Enabled (mapped to CIS Controls v8.1.2 safeguard 4.4, CMMC L1/L2, NIST SP 800-53 Rev. 5, and Microsoft Cloud Security Benchmark v1) and Distributed Table Without Diagnostic Logging, requiring the `allLogs` category. Expands the Azure Diagnostic Settings harvester to collect diagnostic settings for Cosmos DB accounts (`Microsoft.DocumentDb/databaseAccounts`) and the Distributed Table harvester to collect the `public_network_access` property.

— Named filters, insights, resource type and compliance mappings, no direct API call

2026-09-15-3c05e607

03 **Database Instance security checks across PostgreSQL, SQL Server, MySQL**

NEW

80

Adds `Database Instance Entra-Only Authentication` Query Filter to identify Database Instances without Microsoft Entra-only authentication configured. Adds Insights: Database Instance Without Microsoft Entra-Only Authentication (PostgreSQL); Database Instance Public Network Access Enabled (SQL Server); Database Instance Without Secure Transport Enabled (MySQL), detecting Azure Database for MySQL Flexible Servers where `require_secure_transport` is not enabled; and Database Instance Without Connection Log Auditing Events (MySQL), detecting instances where `audit_log_events` does not include `CONNECTION` or `CONNECTION_V2`, aligned with CIS Azure Database Services Benchmark v2.0.0 Control 5.6. Expands the Azure Database Instance harvester to collect Microsoft Entra-only authentication status for Azure Database for PostgreSQL flexible servers.

— Names four insights, one filter, two config fields, and CIS control mapping

2026-09-15-3c05e607

WAS THIS USEFUL? 👍 👎

Plerion

Feedback ⓘ 1 RELEASE · 2026-09-15 NOTES ↗ RANK

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

> Plerion added enterprise identity and access controls this window: SCIM 2.0 provisioning, syncable user groups, organization-scoped API keys, and break-glass admin accounts.

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

01 **SCIM 2.0 provisioning support** NEW 65

Plerion adds SCIM 2.0 provisioning so Okta, Microsoft Entra ID, or any SCIM 2.0 identity provider can create, update, and deactivate Plerion users. Existing users are matched by email address and adopted automatically into the SCIM-managed set.

— Names identity providers and matching logic but no exact setup steps.

SCIM provisioning:

02 **Organization-scoped API keys** NEW 60

Adds organization API keys scoped to the whole organization with `read` or `readWrite` access, intended for use by identity providers performing SCIM provisioning.

— Names concrete access levels but no endpoint or generation flow. SCIM provisioning:

THINNER COVERAGE BELOW

03 **Break-glass admin accounts** NEW 45

Organization admins can be designated as break-glass accounts that can always sign in with a password and cannot be deactivated by an identity provider; at least one is required when SSO or SCIM is enabled.

— Describes the safeguard's rules without setup instructions. SCIM provisioning:

04 **User groups with role inheritance** NEW 40

New user groups grant roles to every member, and can be synced from an identity provider over SCIM or created directly within Plerion.

— Explains behavior but gives no concrete creation or config path. SCIM provisioning:

WAS THIS USEFUL? 👍 👎

◆ Container & Image Security

kata-containers

Feedback ⓘ 1 RELEASE · 2026-09-15 NOTES ↗

RANK

Kata Containers is an open source project and community working to build a standard implementation of lightweight Virtual Machines (VMs) that feel and perform like containers, but provide the workload isolation and security advantages of VMs. https://katacontainers.io/

> Kata Containers 4.2.0 adds TLS to the monitoring endpoint, moves block and VFIO device attachment in the QEMU runtime to file-descriptor passing, and removes two unsupported runtime-rs config overrides.

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

01 **Removed unsupported runtime-rs config overrides** BREAKING

70

The `disable_block_device_use` option is removed from `runtime-rs` as it was unsupported — configs referencing it will need to be updated. The `cpu_nested_config` override is removed from `runtime-rs`.

— Names exact config keys and migration need 4.2.0

02 **FD-based block and VFIO device passing in runtime-rs/QEMU**

NEW

65

Passes block storage sources by file descriptor in `runtime-rs/QEMU`, enabling more secure and flexible block device attachment, and passes VFIO devices by file descriptor in `runtime-rs/QEMU`, enabling fd-based VFIO device handoff.

— Names mechanism and scope but no config flag 4.2.0

THINNER COVERAGE BELOW

03 **NVIDIA GPU guest image enhancements** NEW

55

Ships `dcgm-exporter` in the NVIDIA GPU guest images and enables NFD (Node Feature Discovery) in the NVIDIA kata-deploy presets.

— Names two concrete additions, no usage steps 4.2.0

04 **Cold-plug block devices with Cloud Hypervisor** NEW

50

Enables cold-plug of block devices requested before boot in `runtime-rs` with Cloud Hypervisor.

— Names runtime and hypervisor, no config detail 4.2.0

05 **virtio-rng entropy device in dragonball VMM** NEW 45

Adds `virtio-rng` entropy device to the dragonball VMM.

— Names the device and VMM, no further detail 4.2.0

06 **Rootfs base bumped to Ubuntu 26.04** IMPROVED 45

Bumps rootfs base to Ubuntu 26.04 across all images.

— Names the version but no rationale or impact 4.2.0

07 **TLS support for kata-monitor** NEW 40

Adds TLS support to `kata-monitor` for encrypted metrics exposure.

— Names the component but no flag or config key given 4.2.0

08 **Early guest console log capture** NEW 40

Captures early guest console logs in the runtime before the agent is fully up.

— Explains behaviour but no interface named 4.2.0

09 **CLH nested virtualization disable option** NEW 40

Allows disabling CLH nested virtualization in the runtime.

— Names capability but not the exact flag 4.2.0

└──▷ **BREAKING ON UPGRADE**

! The `disable_block_device_use` option is removed from `runtime-rs` as it was unsupported — configs referencing it will need to be updated.

! The `cpu_nested_config` override is removed from `runtime-rs`.

WAS THIS USEFUL? 👍 👎

DETECTION & RESPONSE

◆ SIEM

Databricks

Feedback ⓘ 4 RELEASES · 2026-09-09 → 2026-09-15 BLOG ↗

RANK

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

> Databricks shipped a Beta snapshots API for Lakebase, session restore for debugging failed serverless jobs, an audio transcription AI function, Slack-embedded Genie visualizations, and configurable retention for system tables.

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

01 **Lakebase snapshots API** NEW 75

A Beta API for Lakebase supports `create`, `get`, `list`, and `delete` operations on point-in-time snapshots of a project branch, plus restoring a snapshot by creating a new branch from it.

— Names operations but no request paths or SDK syntax

Lakebase snapshots API (Beta) (2026-09-…

02 **Session restore for serverless jobs** NEW 75

Public Preview feature that automatically captures a snapshot of Python variables and Spark session state from eligible serverless compute job runs, letting you restore them into a new interactive notebook to debug failures or explore results without rerunning the entire job.

— Explains mechanism and workflow, no exact UI steps

Session restore for serverless jobs is …

03 **ai_transcribe audio transcription function** NEW 75

New `ai_transcribe` SQL/AI function transcribes audio files to text, producing per-segment timestamps and automatic speaker labeling.

— Named function usable directly in SQL, thin on parameters product docs

THINNER COVERAGE BELOW

04 **Configurable retention for system tables** NEW 55

Account admins can now set a data retention period between 30 and 3,650 days for supported system tables account-wide (Beta).

— Gives concrete range and role but no config key or command

Configurable retention for system table…

05 **Genie chart visualizations in Slack replies** NEW 45

Genie chart visualizations now render as inline images directly in Slack replies when using the Databricks Genie app for Slack (Public Preview).

— Describes the behavior but no setup or config detail

Genie visualizations in Slack replies (…

WAS THIS USEFUL? 👍 👎

◆ Detection Engineering

Tenzir

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

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

> Tenzir shipped performance improvements to its pipeline engine, on-demand schema loading in the platform, and automatic Sigma rule matching for OCSF-formatted events.

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

01 **Automatic Sigma matching for OCSF events** NEW 50

Tenzir Node v6.16.0 adds automatic Sigma rule matching for OCSF-formatted events, extending detection coverage to OCSF schemas without manual mapping.

— Names the schema and mechanism but no exact command or flag.

changelog-20260915-989167dd

02 **Parallel data movement and deeper operator pushdown** IMPROVED 35

Tenzir Node v6.17.0 adds parallel data movement and deeper operator pushdown to accelerate pipeline throughput.

— No mechanism or benchmark given, just named version and terms.

changelog-20260915-989167dd

03 **On-demand schema loading in Platform** IMPROVED 30

Tenzir Platform v1.39.2 adds on-demand schema loading, enabling schemas to be fetched as needed rather than preloaded.

— Describes behavior change but no config or command to invoke it.

changelog-20260915-989167dd

WAS THIS USEFUL? 👍 👎

◆ Managed Detection & Response (MDR)

Arctic Wolf

Feedback ⓘ 1 RELEASE · 2026-09-15 BLOG ↗ RANK

Instinct meets AI. Arctic Wolf Aurora's built-in agents operate at machine speed while human experts maintain oversight.

> Arctic Wolf introduced Aurora MDR Connect, a new managed detection and response tier built exclusively for MSPs.

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

01 **Aurora MDR Connect for MSPs** NEW 30

A new tier of Aurora Managed Detection and Response built exclusively for MSPs, powered by the Aurora Superintelligence Platform and the Aurora Agentic SOC.

– Names the tier and platform but no mechanism or how MSPs use it.

Introducing Aurora® MDR Connect: A New …

WAS THIS USEFUL? 👍 👎

EXPOSURE & VULNERABILITY MANAGEMENT

◆ Attack Surface & Exposure Management

Censys

Feedback ⓘ 1 RELEASE · 2026-09-14 BLOG ↗ RANK

Censys is a search engine for internet-connected devices and certificates, enabling security researchers to discover and analyze exposed assets.

> Censys added case-insensitive regex matching to its query language, rolled out 22 new protocol and application scanners, and added two ASM risk fingerprints for recent GitLab vulnerabilities.

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

01 **Case-insensitive regex in CenQL** NEW 80

Adds the (?i) case-insensitive regex operator to the Censys Query Language (CenQL), enabling case-insensitive `value=~` pattern matching in fields such as `host.services.endpoints.http.headers` and other string fields.

Hunt for nginx servers advertised with non-standard casing (e.g. `Nginx`, `NGINX`) to catch assets that evade case-sensitive filters.

```
$ host.services.endpoints.http.headers:(key="Server" and value=~"(?i)^nginx$" and not value="nginx")
```

— Names exact operator and field, includes runnable query September 14, 2026 (2026-09-14)

02 **New ASM risk fingerprints for GitLab CVEs** NEW 80

Adds two new ASM risk fingerprints queryable via `risks.name`: `Vulnerable GitLab Server (CVE-2026-85706)` covering unauthenticated arbitrary file read via the repository commits API, and `Vulnerable GitLab Server (CVE-2026-87719)` covering authenticated credential leak via a GraphQL subscription in GitLab EE.

Query ASM for assets flagged as vulnerable to the unauthenticated GitLab arbitrary-file-read risk to prioritize patching.

```
$ risks.name: "GitLab Server (CVE-2026-85706)"
```

— Names CVEs, mechanism, and runnable query field September 14, 2026 (2026-09-14)

03 **22 new protocol and application scanners** NEW 60

Adds 22 new protocol, application, and endpoint scanners to the Platform: `UTILINET_LPP`, `ORENCO_ATRTU`, `OPW_FSC3000` (Critical Infrastructure module);

`PIGEONHOLE`, `SAMSUNG_OFFICESERV`, `CISCO_SDWAN_VDAEMON`, `VANTAGE_INFUSION`, `CNORD_SECURITY_CENTER`, `VISIONHITECH_IPCAM` (Starter/Search/Core); and `OTLP_GRPC`, `NETFLIX_NRDP`, `HIKVISION_DNVRS`, `SPOTIFY_CONNECT`, `MANAGESIEVE`, `LIBP2P`, `TAURUS_STB`, `GEOVISION_AUDIO`, `BLUEMAX_NUTTCP`, `WOW_REALMD`, `THRULAY`, `STOMP`, and `CLAMAV` (available to all users).

— Names all 22 scanners but no usage example given `September 14, 2026 (2026-09-14)`

WAS THIS USEFUL? 👍 👎

◆ Vulnerability Management

defectdojo

Feedback ⓘ 1 RELEASE · 2026-09-14 NOTES ↗ RANK

Open-Source Unified Vulnerability Management, DevSecOps & ASPM

> DefectDojo added inline image support to the Markdown editor for finding notes and reports, and extended the deduplication engine with configurable candidate scope, winner ordering, and dedupe pools.

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

01 Inline images in Markdown editor NEW

63

The Markdown editor used in Finding notes, descriptions, and other markdown fields now supports images via paste from clipboard, drag-and-drop, or the Insert image toolbar button. Images are stored by DefectDojo and render inline in the notes feed and in generated reports, removing the need for an external image host.

Attach a screenshot of exploit evidence directly to a finding note so it appears inline in reports without needing an external host.

> 📍 In a Finding, open the Notes section, then paste a screenshot from your clipboard or drag an image file onto the Markdown editor. The image is stored by DefectDojo and rendered inline in the notes feed and any generated reports.

— Names UI mechanism and toolbar button, but no config surface. product docs

THINNER COVERAGE BELOW

02 Configurable deduplication engine scope and pools IMPROVED

35

The deduplication engine gains injectable candidate scope and winner order configuration, along with support for dedupe pools.

— Names mechanism but no concrete config keys or examples. 3.3.100

WAS THIS USEFUL? 👍 👎

IDENTITY, ACCESS & DATA PROTECTION

◆ Data Security & DLP

Immuta

Feedback ⓘ 1 RELEASE · SEEN 2026-09-15 NOTES ↗ RANK

Use Immuta to provision governed access to data.

> Immuta's Request app now supports submitting a single access request for multiple users, while fingerprint-based masking options for Snowflake are being deprecated ahead of removal in December 2026.

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

01 Fingerprint-based masking deprecated for Snowflake DEPRECATED

60

Fingerprint-based masking options — format-preserving masking, randomized response masking, and rounding/grouping using a data fingerprint — for Snowflake integrations are deprecated and will be removed from Immuta SaaS on December 15, 2026. Tenants without existing policies using these options can no longer create new ones.

— Names exact masking types, integration, and removal date. snapshot-20260915

THINNER COVERAGE BELOW

02 Multi-user access requests in Request app NEW

52

The Immuta Request app now lets managers and admins select multiple users in a single request form and submit once instead of once per user. The form also adds an email address hover-over on user names to help distinguish between users with similar or identical names.

Request access for an entire team in one submission rather than repeating the process for each individual.

> 📍 In the Immuta Request app, open the request form, select all relevant users from the user list, fill in the request details, and click Submit once to create a single access request covering all selected users.

— Clear behavior and UI steps given, but no config/API name. snapshot-20260915

└──▷ BREAKING ON UPGRADE

! Fingerprint-based masking options (format-preserving masking, randomized response masking, and rounding/grouping using a data fingerprint) for Snowflake integrations are deprecated and will be removed from Immuta SaaS on December 15, 2026. Tenants without existing policies using these options can no longer create them.

WAS THIS USEFUL?  

Varonis

Feedback

8 RELEASES · 2026-08-23 → 2026-09-15

CHANGELOG ↗

RANK

The leading data and AI security platform that proactively reduces risk, enforces policies, and stops active threats with our AI-native automation.

> Varonis expanded its web interface to cover core administrative workflows (dictionaries, users/roles, permissions/groups) that previously required the separate Management Console, while also adding a unified account activity view, non-human identity monitoring in Entra ID, SharePoint sensitivity-label filtering, and custom link prefixes for Data Lifecycle Automation.

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

01 Web interface administration for dictionaries, users, and permissions

NEW

68

Consolidates administration previously requiring the Management Console into the Varonis web interface: creating and updating dictionaries alongside EDM classifiers and classification policies; creating, viewing, and managing users and roles; and managing permissions, groups, folder protection, and memberships directly from the Analytics page.

— Names every consolidated admin surface but only points to UI, not a specific flow

Manage permissions and groups directly … | Manage dictionaries directly in the Var… | Manage Varonis users and roles from the… | changelog-20260915-5335c785

02 Unified account activity investigation in Account Pane NEW

63

Adds a dedicated Activity tab inside the Account Pane that combines activity trends and detailed event logs in a single view, with interactive filtering and drill-down to identify spikes and accelerate investigations.

When an alert fires on a user account, open the Account Pane and navigate to the Activity tab to see event trends and drill into specific events without leaving the pane.

> 📍 In the Varonis console, locate the account in question and open the Account Pane › Activity tab. Use the interactive filters to narrow by time range or event type, then drill down into spikes to review detailed event logs.

Quickly triage unusual account behavior during an incident by reviewing activity trends and raw event logs without pivoting between screens.

📍 In the Varonis web interface, open the Account Pane for the account under investigation, select the Activity tab, use the interactive filters to isolate the relevant time window, and drill down into event log entries showing the spike.

— Names exact UI location and includes step-by-step usage example

Investigate account activity from a sin… | changelog-20260915-5335c785

THINNER COVERAGE BELOW

03 **SharePoint site filtering by sensitivity label** NEW

40

Enables filtering and analysis of SharePoint Online sites by sensitivity label assigned directly to the site, surfacing site-level classification for security and compliance investigations.

— Describes capability but no concrete steps or UI path given

Filter and analyze SharePoint sites but…

04 **Custom link prefixes for Data Lifecycle Automation** NEW

40

Data Lifecycle Automation policies can now generate links with custom prefixes when content is moved, making automation-generated links distinguishable for auditing and link management.

— Explains the mechanism but gives no configuration steps

Identify links generated by Data Lifecy…

05 **Non-human sign-in monitoring in Entra ID** NEW

40

Monitors and surfaces authentication events for service principals and AI agents in Entra ID, enabling investigation of non-human identity sign-ins that were previously invisible.

— Clear capability description but no path to view or use it

Monitor non-human sign-ins in Entra ID

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

JumpCloud

Feedback ⓘ 8 RELEASES · 2026-09-14 BLOG ↗ RANK

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

> JumpCloud's biggest window moves are new standalone products — Password Vault, Access Requests, the MCP Server, AI Commands Builder, and GA Access Risk Detection — layered on top of steady identity work (JumpCloud Go passwordless login, certificate-based RADIUS, OIDC SSO, forced SAML/OIDC re-authentication) and device management growth across Windows, Android, and Apple MDM, Device Monitoring and Alerting, and a granular Custom Admin Roles/RBAC rework.

└──▷ **WHAT SHIPPED · 51 FEATURES** most completely described first ? what's the number?

01 **AI & SaaS Management platform** IMPROVED 93

Introduces SaaS Management with discovery, categorization, warning/blocking controls, and usage insights for shadow IT apps via the JumpCloud Go browser extension, and lets admins manually add applications for tracking, warning, and blocking before automatic discovery occurs (r2). Renames it to AI & SaaS Management and significantly expands coverage of generative AI apps for discovery, adds the Shadow AI Dashboard for visibility into generative AI shadow IT usage, adoption by department, and most active users, and releases SaaS License Management to GA, automating license tracking for supported SaaS applications via connectors (r3). Adds `MCP Discovery` and `Token & Cost Tracking` options under `Access > AI & SaaS Management > Settings > Enhanced Discovery Options` to discover MCP servers and track token usage and estimated cost from Cursor, Claude Code, OpenCode, Codex, and VS Code Copilot CLI on managed Windows and macOS devices, and adds an `MCP Connection` column in `Access > AI & SaaS Management > Applications` showing `Discovered`, `Connected`, or `Not Available` status for each app, with `Add MCP Server` and `View` actions available inline (r4).

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

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

Connect a discovered MCP server to AI Gateway from the same view used to manage SaaS apps, without switching tools.

📍 In the Admin Portal, go to Access › AI & SaaS Management › Applications. Locate an app showing Discovered in the MCP Connection column, click the status, review the discovered MCP servers, and click Add MCP Server.

— Every setting path and column name is named verbatim. Release Notes 2026 (2026-09-14) Release Notes 2025 (2026-09-14) Release Notes 2024 (2026-09-14)

02 **Custom Admin Roles with granular RBAC scopes** BREAKING

90

Releases Custom Admin Roles for all direct organizations, enabling granular role creation based on specific admin responsibilities (r3). Adds CRUD operations and a No Access permission to the Identity Management and Application Management scopes; splits Identity Management and Directory and Groups Management into separate, independently assignable scopes; moves Directory Management and Group Management under a unified Directory and Groups Management category, SaaS Applications and Asset Management under SaaS and Asset Management, and RADIUS Authentication under Access Management; includes Application Templates in the Applications scope and existing User Portal APIs/operations under the Multi-Factor Authentication scope; and renames Policy Management to Access Management, System Management to Devices, and Authentication Policies to Conditional Access Policies and IP Lists (r5 preview).

— Names every renamed and reorganized scope for migration.

Roles Based Access Release Notes 2025 (… Release Notes 2025 (2026-09-14)

03 **API deprecations: reactivate endpoint and Dynamic Groups filter operators**

DEPRECATED

88

The `GET` request for `api/systemusers/reactivate/{id}` is deprecated and now returns a 404 error; replace it with `POST https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body. Dynamic Groups API `memberQuery` filter operators `$ge` and `$le` are deprecated and replaced by `$gte` and `$lte`; existing API scripts using `$ge` or `$le` must be updated.

— Gives exact old and new endpoints/operators to migrate. Release Notes 2024 (2026-09-14)

04 **Forced re-authentication and authentication method claims**

NEW

83

Adds forced re-authentication support: the IdP now honors `ForceAuthn="true"` in SAML and `prompt=login` in OIDC, prompting users for credentials even with an active session; and adds Authentication Methods References (AMR) claims in both SAML

assertions and OIDC ID tokens, tagging logins with proof of factors used (e.g., password + OTP).

Trigger step-up authentication for a high-privilege app by sending a SAML AuthnRequest with ForceAuthn set, ensuring the user must re-authenticate even with an active session.

```text
<samlp:AuthnRequest ... ForceAuthn="true" ...>...
</samlp:AuthnRequest>
```

— Exact protocol parameters and a runnable SAML example. Release Notes 2025 (2026-09-14)

---

05 **Patch management for macOS and browsers** NEW 80

Adds per-device macOS software update scheduling from the Admin Portal, including timeframe control and user deferral options; adds macOS Ventura upgrade-blocking software management policies so admins can delay or prevent unwanted upgrades to macOS 13; adds a Managed Login Items policy for macOS 13 Ventura to prevent end users from disabling persistent software such as the JumpCloud Agent; adds a Universal Browser Patch Management policy for Google Chrome across macOS, Windows, and Linux from a single policy; and adds a Browser Patch Management Policy Report and an OS Patch Management Policy Report for audit evidence and compliance status.

Prevent macOS 13 Ventura from upgrading automatically on managed devices while you validate app compatibility.

> 📍 In the Admin Portal, go to Device Management › Policies › New Policy, select the macOS Ventura delay/block software management policy, configure the deferral window, and bind it to your macOS device groups before the delta update is offered.

— Names each policy and report with example steps. Release Notes 2022 (2026-09-14)

---

06 **Password Manager storage limits and auto-lock controls**

IMPROVED 78

Raises item storage limits to 13,000 items with autofill enabled, 5,000 items per shared folder, and 30,000 items when autofill is not used; introduces an auto-lock schedule with a default of 15 minutes of inactivity and a maximum of 1440 minutes (24 hours), plus an Auto Lock setting that locks the app when the device is locked.

— Exact limits and timeout defaults given, no toggle path.

What's New: Password Manager Desktop Ap…

---

07 **MFA and JumpCloud Protect hardening** IMPROVED 78

Enables MFA by default for all new admin accounts logging into the Admin Portal, splits WebAuthn into separate Security Keys and Device credential types for enrollment, adds push bombing mitigation for JumpCloud Protect blocking more than one notification per resource within a sixty-second period (configurable in MFA Configurations), and adds lock-screen push notification approval or denial in JumpCloud Protect (long-press on iOS, expand on Android) when User Verification is not required (r1). Allows admins to enable password resets from the User Portal when MFA is enforced but the user has not yet enrolled (r2). Adds user group exclusion from JumpCloud Protect Push enforcement, allowing excluded groups to use TOTP only (r3).

Harden admin push notification security by reviewing the sixty-second push bombing limit and adjusting the maximum concurrent attempts for your org.

> 📍 In the Admin Portal, go to Security › MFA Configurations, locate JumpCloud Protect push settings, and adjust the maximum concurrent attempts or disable the limit.

— Names configurable threshold and exclusion mechanism. Release Notes 2025 (2026-09-14) Release Notes 2024 (2026-09-14) Release Notes 2023 (2026-09-14)

---

08 Multi-Tenant Portal administration features IMPROVED

77

Adds MSP admin ability to bulk-select and export reports across all tenant organizations as JSON or CSV from the Multi-Tenant Portal homepage, and adds MSP Custom Command Templates so MSP admins can create, save, and apply command templates across tenant organisations (r0). Adds ad hoc command execution on devices directly from the Multi-Tenant Portal and Admin Portal, the ability to add new users and devices, export user and device lists, and run bulk actions directly from the Multi-Tenant Portal, and MSP billing visibility for committed user license counts and JumpCloud contract downloads (r1). Adds `Account > Settings > Global MFA Requirement` in the Multi-Tenant Portal to bulk-enforce MFA for all MSP admins in a tenant (r2).

Enforce MFA for every MSP admin in your tenant from the Multi-Tenant Portal without touching individual admin accounts.

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

— Names exact toggle path and export formats. Release Notes 2024 (2026-09-14) Release Notes 2023 (2026-09-14) Release Notes 2022 (2026-09-14)

---

09 Dynamic Groups for devices and users NEW

77

Adds Dynamic Groups for both devices and users, allowing admins to automate group membership via attribute-based rules with optional pre-review of membership changes;

adds Vendor and Public IP Address as new attributes for dynamic device groups, and Manager as a new attribute for dynamic user groups.

Automatically maintain a device group of all macOS endpoints from a specific vendor so policies stay current as fleet changes.

> 📍 In the Admin Portal, go to Device Groups, create or edit a group, enable Dynamic, and add a rule: Attribute = Vendor, Operator = is, Value = Apple.

— Exact attribute names and a rule example given. Release Notes 2023 (2026-09-14)

---

10 **Shared folder management in Password Manager** IMPROVED

76

Adds shared folder management for JumpCloud Password Manager from the Admin Portal, including manual per-folder sync from the desktop application (r1); admins can create and update shared folders and assign users or user groups to any shared folder, a Move All items button moves every item in a folder at once, and shared folder events sync to Directory Insights (r7).

Assign a user group to a shared folder so the whole team gets access to shared credentials without manual per-user assignment.

> 📍 In the Password Manager desktop app, go to Shared Folders, select or create a folder, then use Assign Users or User Groups to add the relevant group.

Bulk-relocate all credentials out of a shared folder in one action when reorganizing vault structure or offboarding a team.

> 📍 Open the shared folder in the Password Manager desktop app, then click the Move All items button to move every item in the folder at once.

— Names exact UI actions and Directory Insights sync target.

What's New: Password Manager Desktop Ap… Release Notes 2023 (2026-09-14)

11 **JumpCloud Go passwordless authentication** IMPROVED 76

Adds the `JumpCloud Go` browser extension enabling hardware-protected, phishing-resistant passwordless login using Apple Touch ID and Windows Hello on managed macOS and Windows devices, and enforces it as the default MFA method for conditional access policies on SSO apps with user and device verification on every application session (r1). JumpCloud Go sessions now automatically refresh on device login or unlock, enabling seamless access to protected resources without additional MFA challenges, and a new `User Portal > Security > Multi-Factor Authentication` section lets users manage JumpCloud Go sessions per device (r2).

— Names exact User Portal path, mechanism explained. Release Notes 2024 (2026-09-14) Release Notes 2023 (2026-09-14)

12 **Access Risk Detection reaches general availability** NEW 75

Promotes Access Risk Detection to general availability, providing behavior-based detection of unusual locations, impossible travel, unfamiliar devices, dormant accounts, and abnormal login volumes, with configurable risk factors, automatic MFA-based resolution, intelligent VPN/gateway suppression, and email, Slack, and webhook notifications.

— Rich mechanism list but no config path given. Release Notes 2026 (2026-09-14)

13 **Commands feature: agent-install triggers, running status, remote tools**

NEW 74

Adds a Command After Agent Install command type so admins can specify enrollment commands to run immediately after the JumpCloud agent is installed on new devices, and adds a Running column to the commands queue to distinguish commands waiting in queue from commands actively running (r0). Adds Background Tools remote command line and remote file transfer capabilities, letting admins access an end-user's device and transfer files without disrupting their work (r1).

Enroll new Windows endpoints with a hardening script that runs the moment the JumpCloud agent finishes installing, before any user logs in.

> 📍 In the Admin Portal, go to Commands › New Command, set the command type to Command After Agent Install, paste your hardening script, and save — the command will execute automatically on every newly enrolled device.

— Names command type and queue column, with a setup example.

Release Notes 2023 (2026-09-14) Release Notes 2022 (2026-09-14)

14 **MCP servers require SSO application association in AI Gateway**

73

BREAKING

MCP servers in AI Gateway must now be associated with an SSO application or bookmark via the `App` dropdown, enabling group-based access scoping; a `+ New App` option opens the standard Add New SSO Application wizard during server setup. Previously created MCP servers without an associated application must be assigned one or access will not be scoped by User Groups.

— Names exact dropdown and migration requirement. Release Notes 2026 (2026-09-14)

15 **Remote Assist remote support** NEW 73

Introduces JumpCloud Remote Assist for unlimited remote desktop access and support on Windows and macOS — free, installed silently via JumpCloud Agent v1.61.0 or later (r0). Adds user-switching between accounts during Remote Assist sessions on Windows devices, a `Ctrl+Alt+Del` command shortcut from the Session Options toolbar, and support for viewing and interacting with the initial login screen on Windows servers (r1). Ships Remote Assist as two separate architecture-specific packages — `ARM64` for Apple Silicon and `x86_64` for Intel Macs (r2).

— Names agent version and packages, no launch command. Release Notes 2024 (2026-09-14)

Release Notes 2023 (2026-09-14) Release Notes 2022 (2026-09-14)

16 **RADIUS authentication enhancements** IMPROVED 72

Adds certificate (passwordless) based authentication to JumpCloud RADIUS, supporting any X.509 compliant certificate authority — existing certificates can be imported and used for RADIUS auth; adds RADIUS authentication with Azure AD as the identity provider, enabling secure RADIUS access without managing users outside Azure AD (r0). Adds faster reconnect for EAP connections by allowing recently authenticated devices to skip the full security handshake using a cached session credential (r3).

— Explains certificate import and cached-credential mechanism.

Release Notes 2025 (2026-09-14) Release Notes 2022 (2026-09-14)

17 **Agent Identities for AI Gateway** NEW 70

Introduces Agent Identities so admins can register an AI agent with OAuth client credentials for the JumpCloud AI Gateway and scope its SSO application access via Agent Groups, keeping automated agents auditable and separate from human accounts.

Register an AI agent identity with OAuth credentials and scope its SSO application access via a group, keeping it auditable and separate from human accounts.

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

— Full setup example given, but no bullet describing limits.

Release Notes 2026 (2026-09-14)

---

18 **API filter escaping for pipe character** IMPROVED 70

Adds support for escaping the pipe `|` character with backslash `\\` inside `in` and `nin` API filter operators (e.g. `GET /systemusers?filter=department:$in:...`), enabling pipe characters in search terms.

— Names exact endpoint and escape syntax. Release Notes 2024 (2026-09-14)

---

19 **Admin-managed Password Manager install via command template v2.0.0**

IMPROVED 69

Admins can install and update the Password Manager desktop app using a new command template `v.2.0.0` on Windows and macOS devices, removing the need for users to have admin permissions for subsequent updates.

— Names exact template version and platforms. What's New: Password Manager Desktop Ap…

---

20 **Password Manager Desktop App platform builds expand** NEW 68

Adds a Password Manager Desktop App Linux build (Debian/Ubuntu x86) with improved security and automatic updates (r1); adds an ARM build for macOS devices with M-series silicon (M1 and above), available on the Downloads page with automatic update to the ARM build when applicable, and an RPM build for Linux (x64 Red Hat distributions such as Fedora), auto-updating and stable, alongside the existing Debian build (r7).

— Names exact build targets but no install command.

What's New: Password Manager Desktop Ap… Release Notes 2023 (2026-09-14)

---

21 **Asset Management enhancements** NEW 68

Adds an Asset Manager role in the Admin Portal providing dedicated Asset Management access without broader admin permissions; adds file upload functionality (Invoice field) to asset records under Purchase Details with support for custom fields of the File Upload type; adds Disk Size to Hardware Specifications for tracking device storage capacity; adds a Local Device Accounts display on the Asset Detail page under Device Management; and adds asset cloning, automatically clearing unique fields to prevent duplicates.

— Names each field and location, no exact click path. Release Notes 2025 (2026-09-14)

---

22 **Access Requests approval workflow** NEW 67

Introduces JumpCloud Access Requests, enabling approval flows for access requests submittable from the JumpCloud User Portal and manageable in the admin console; adds webhook support to integrate with external ticketing systems such as JIRA,

automatically creating tickets on new request submission; and tracks Access Request events in Directory Insights.

— Names webhook and Directory Insights integration, no config key.

Release Notes 2025 (2026-09-14)

23 **Support case portal evolves into Customer Portal** IMPROVED

65

Adds the JumpCloud Case Portal under the Support menu, centralising all organisation cases and ideas into a filterable list with clickable case numbers (r0). Introduces the Customer Portal for tracking and managing support cases, with sortable columns for Last Modified Date, Account, and Requester, plus attachment uploads and inline ticket editing, and adds MTP admin access to view and create support cases for all managed tenant organizations (r3).

— Names sortable columns but no exact menu path. Release Notes 2025 (2026-09-14)

Release Notes 2022 (2026-09-14)

24 **Android MDM management: zero-touch, EMM, work profile** NEW

65

Adds Android zero-touch enrollment support for fully managed, dedicated, and company-owned Android devices with a work profile (r1); adds Android EMM support for fully managed and dedicated devices with 7 new policies including Factory Reset Protection, Kiosk Mode, and System Updates, plus Android EMM work profile support for enrolling and managing company-owned and personal Android mobile devices (r1); and adds full Android 15 support in MDM (r2).

— Names policy examples, no navigation path. Release Notes 2024 (2026-09-14)

Release Notes 2023 (2026-09-14)

25 **Apple MDM enrollment, restriction policies, and app deployment**

NEW

65

Supports BYOD enrollment of iOS/iPadOS 18+ devices via Account-Driven User Enrollment (ADUE) in MDM, now in general availability, and adds two new MDM policies to restrict Apple Intelligence features on iOS/iPadOS 18.1 and macOS 15.1 Sequoia devices (r2). Adds Apple Business Manager as a new service discovery method for Account-driven Enrollment, and adds IPA file support to the JumpCloud Private Repository for uploading and deploying iOS and iPadOS app packages (r3).

— Names exact OS versions and policy targets. Release Notes 2025 (2026-09-14)

Release Notes 2024 (2026-09-14)

26 **Windows App Catalog** NEW

65

Launches JumpCloud App Catalog for Windows, enabling install and auto-update management for 1Password, Adobe Acrobat Reader DC, Chrome, Firefox, Google Drive, OneDrive, OpenVPN, Slack, Webex, and Zoom.

— Names every supported app, no policy assignment steps. Release Notes 2024 (2026-09-14)

27 **Third-party integrations: SentinelOne, AWS Verified Access, Deel, Microsoft 365**

NEW 65

Adds SentinelOne integration via the Commands feature to download and install the SentinelOne Agent on macOS, Windows, and Linux devices, and extends the Microsoft 365 integration to include M365/Azure AD security groups (r0). Adds integration with AWS Verified Access using JumpCloud Go, SAML, or OIDC SSO as a VPN-less remote access solution, and adds a Deel SSO Connector integration (r1).

— Names each integration, no setup steps for most. Release Notes 2023 (2026-09-14) Release Notes 2022 (2026-09-14)

28 **Password Manager Desktop App usability and list management**

IMPROVED 62

Adds Download Logs and Keyboard Shortcuts options under Settings, and multi-select functionality with item sorting (r2); extends sorting to various criteria including nicknames, adds multi-select for bulk management, a paginated items list showing 100 items per page, a Copy button in Password History, ability to delete multiple folders at once, a What's New link on Settings > General for release updates, and archiving of items with the ability to view, delete, and restore archived items (r7).

— Lists many UI additions but no config surface. What's New: Password Manager Desktop Ap… Release Notes 2024 (2026-09-14)

29 **Device Monitoring and Alerting** NEW 62

Introduces JumpCloud Device Monitoring and Alerting, supporting availability, software, uptime, disk, and battery monitoring plus directory event alerts (user addition, privilege elevation) on Windows, macOS, and Linux endpoints.

— Lists monitored metrics, no threshold configuration shown. Release Notes 2024 (2026-09-14)

30 **Windows MDM CSP policy and SCEP expansion** NEW 62

Adds six new Windows MDM CSP-based policies: Windows Wi-Fi Configuration Policy, Windows VPN Policy, Install Certificate Policy, Bluetooth Configuration Policy, Control Policy Conflict, and Windows Notification Service, plus a new policy to configure Simple Certificate Enrollment Protocol (SCEP) for Windows devices.

— Names every policy verbatim, no assignment walkthrough. Release Notes 2024 (2026-09-14)

31 **MDM/SSO certificate and token expiration monitoring** IMPROVED

61

Adds an MDM Upcoming Certificate Expirations homepage widget covering MDM certificates, Apple VPP, and Automated Device Enrollment Certificates (r0), evolving into an MDM Certificate & Token Status Board on the Admin Portal and Multi-Tenant Portal homepages, showing expiry status for MDM, SSO, and AzureAD tokens and certificates with an aggregate MSP view (r1).

— Names each cert/token type tracked, no alert config given.

Release Notes 2023 (2026-09-14) Release Notes 2022 (2026-09-14)

32 **Linux platform support and hardening** NEW

60

Adds JumpCloud agent support for Linux Fedora 37, and adds a Linux Forbidden Services policy to remove unsupported service types and reduce security risk across Linux fleets.

Block an entire Linux fleet from running unnecessary services (e.g. telnet, rsh) to reduce the attack surface without touching each machine individually.

> 📍 In the Admin Portal, go to Device Management › Policies › New Policy, select Linux Forbidden Services, choose the service types to forbid, and bind the policy to the target Linux device group.

— Names the OS and policy, with a runnable example. Release Notes 2022 (2026-09-14)

THINNER COVERAGE BELOW

33 **Self-Service Account Provisioning** NEW

57

Adds Self-Service Account Provisioning so new users can bind their account to JumpCloud-managed macOS and Windows devices directly from the login window, including a new macOS login window with wireless connectivity controls.

— Describes mechanism, no exact activation steps. Release Notes 2023 (2026-09-14)

34 **Password Manager launch and cloud backup** NEW

56

Introduces JumpCloud Password Manager with end-to-end encrypted local storage, browser extension auto-fill, secure password sharing, and password generation; adds Cloud Backup as a secure fallback to minimize data loss.

— Describes capabilities but gives no setup path or config.

Release Notes 2023 (2026-09-14) Release Notes 2022 (2026-09-14)

35 **RSS feed subscriptions for release notes** NEW

56

Adds RSS subscription options for JumpCloud Help Center updates, including separate feeds for product release notes, agent release notes, and bug fix reports via the Release Notes and Bug Fixes page.

Stay current on JumpCloud product and agent changes by subscribing to the release notes RSS feed in your reader.

> 📍 Go to the JumpCloud Release Notes and Bug Fixes page › Click Subscribe to Release Notes and Bug Fixes RSS Feed › Add the resulting RSS URL to your RSS reader of choice.

— Exact page and subscribe action given. Subscribe to New Feature and Product Up…

---

36 **Password Manager Desktop App drops AppImage build** BREAKING 55

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

— Gives exact deprecation date and required migration target.

What's New: Password Manager Desktop Ap…

---

37 **AI Commands Builder general availability** NEW 55

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

— Names Admin Portal location, no exact navigation path. Release Notes 2025 (2026-09-14)

---

38 **Personalization policies for Windows and macOS** NEW 54

Adds new Windows Personalization policies: Taskbar Customization, Screen Saver Configuration, and Desktop and Lock Screen Settings; and adds new functionality to existing Mac Personalization policies: Dock Settings and Items, and Lock Screen (Screen Saver).

— Names each policy, no config values given. Release Notes 2025 (2026-09-14)

---

39 **Disk encryption device condition in Conditional Access Policies**

NEW 54

Adds disk encryption state (FileVault on macOS, system drive on Windows, root disk on Linux) as a device condition in Conditional Access Policies.

— Names each platform's disk encryption target. Release Notes 2022 (2026-09-14)

---

40 **EU region support for Password Manager** NEW 53

Adds EU region support — users can select their region before activating their account, available on the activation page for the desktop app and on the pairing page for the

browser extension.

– Names exact pages but no data-residency mechanism detail.

What's New: Password Manager Desktop Ap…

41 **User Portal login and application browsing experience** IMPROVED 52

Adds Identity First Login flow for the User Portal and SSO applications, splitting login into a username/email screen followed by a password screen (r0); adds All Applications and Favorites tabs to the Applications area of the User Portal, with a starring mechanism and responsive search field (r1).

– Describes UI flow, no admin configuration path. Release Notes 2023 (2026-09-14)

Release Notes 2022 (2026-09-14)

42 **Directory Insights filter refinement** IMPROVED 48

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

– Names new filter fields, no usage example. Release Notes 2025 (2026-09-14)

43 **LDAP authentication improvements** IMPROVED 48

Adds TOTP as a supported MFA factor for LDAP applications, alongside JumpCloud Protect push notifications (r0); adds source IP tracking for incoming LDAP requests for enhanced security and traceability (r3).

– States factors and tracking without config detail. Release Notes 2025 (2026-09-14)

Release Notes 2022 (2026-09-14)

44 **JumpCloud MCP Server general availability** NEW 47

Introduces the JumpCloud MCP Server (GA), connecting compatible AI tools to JumpCloud via the Model Context Protocol for direct interaction with org data and admin capabilities.

– States purpose without setup steps. Release Notes 2025 (2026-09-14)

45 **Premium Support live chat moves to Admin Portal** BREAKING 45

Adds Premium Support live chat directly in the Admin Portal, automatically recognising Premium Support status without requiring a PIN; live chat is no longer available on the JumpCloud Support site and has moved exclusively to the Admin Portal.

– States relocation, no exact menu path given. Release Notes 2022 (2026-09-14)

46 **Legacy Password Manager CSV export enhancement** IMPROVED

42

Adds enhanced CSV export for the legacy Password Manager with new data fields to support migration to JumpCloud Vault.

— No field names or export path given. What's New: Password Manager Desktop Ap…

---

47 **Admin Portal Cmd/Ctrl+K quick navigation** NEW 40

Adds `Cmd/Ctrl + K` keyboard shortcut in the Admin Portal for quick navigation and search.

— Exact shortcut named, no scope of what's searchable. Release Notes 2024 (2026-09-14)

---

48 **OIDC Single Sign-On support** NEW 38

Adds OpenID Connect (OIDC) Single Sign-On support for OIDC-capable web applications.

— Bare capability statement, no setup steps. Release Notes 2022 (2026-09-14)

---

49 **Service Accounts for APIs** NEW 37

Introduces Service Accounts for APIs, allowing creation of API service accounts not tied to individual admin accounts.

— No creation steps or scope limits given. Release Notes 2025 (2026-09-14)

---

50 **Windows 11 25H2 support** IMPROVED 27

Extends Windows 11 25H2 support across JumpCloud's Windows management components.

— Bare compatibility claim, no specifics. Release Notes 2025 (2026-09-14)

---

51 **Trial recap view** NEW 25

Adds a trial recap view summarising feature usage for admins evaluating JumpCloud trial features.

— Bare description, no location or metrics named. Release Notes 2022 (2026-09-14)

└──▷ BREAKING ON UPGRADE

! Premium Support live chat is no longer available on the JumpCloud Support site — it has moved exclusively to the Admin Portal.

! The `GET` request for `api/systemusers/reactivate/{id}` is deprecated and now returns a 404 error; replace it with `POST` `https://console.jumpcloud.com/systemusers/reactivate/{id}` with `activation_email` in the request body.

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

- ! MCP servers in AI Gateway now require a mandatory association with an SSO application or bookmark; previously created MCP servers without an associated application must be assigned one or access will not be scoped by User Groups.
- ! The `Policy Management` scope is renamed to `Access Management` — any roles or documentation referencing the old name must be updated.
- ! The `System Management` scope is renamed to `Devices` — any roles or documentation referencing the old name must be updated.
- ! The `Authentication Policies` scope is renamed to `Conditional Access Policies and IP Lists` — any roles or documentation referencing the old name must be updated.
- ! Identity Management no longer bundles directory and group permissions; those now live under the separate `Directory and Groups Management` scope — existing custom roles relying on Identity Management for directory/group access must be updated.
- ! JumpCloud Protect is not included in any RBAC scope — admins managing Protect have no RBAC coverage in this release.
- ! The .appimage Linux build is no longer supported as of April 18, 2024; users must migrate to the RPM or Debian build.

WAS THIS USEFUL? 👍 👎

ConductorOne

Feedback ⓘ 1 RELEASE · 2026-09-14 BLOG ↗ RANK

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

> ConductorOne launched an EU data residency instance, giving organizations region-specific URLs across the whole platform, with one known gap in Microsoft Teams support.

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

01 **EU data residency instance** NEW 65

ConductorOne now offers an EU-hosted instance with region-specific URLs for login, API, webhooks, MCP, and CLI, selectable via the Hosting region option (EU) during domain registration. Microsoft Teams as a notification and interaction surface is not yet supported on the EU data residency instance.

When registering a new ConductorOne domain for an EU-based organization, select the EU hosting region so that all tenant URLs (login, API, webhooks, MCP server, CLI) are routed to EU infrastructure.

> 📍 In the ConductorOne domain registration flow, under Hosting region, select EU before completing registration. All tenant-specific URLs — including login, redirect URIs, API and webhook endpoints, MCP server, and CLI configuration — will reflect the EU instance from that point on.

— Names all region-specific surfaces and setup step, but limited mechanism detail.

EU instance (2026-09-14)

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Auth0

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

Secure users, AI agents, and more with Auth0, an easy-to-implement, scalable, and adaptable authentication and authorization platform.

> Auth0 extended Tenant Access Control Lists with a blanket Deny All option that blocks all incoming traffic regardless of signal matching.

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

01 **Deny All rule for Tenant ACL** NEW 70

Adds the `match_all: true` attribute to Tenant Access Control List (ACL) rules, enabling a Deny All rule that rejects all incoming traffic across the full tenant scope without requiring specific signal matching (such as IP or geolocation).

– Names exact config attribute and behavior but no setup steps.

changelog-20260915-92ec9060

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

Nudge Security

Feedback

1 RELEASE · 2026-09-15

CHANGELOG ↗

RANK

Discover every SaaS and AI asset, harden security posture, and scale identity governance.

> Nudge Security expanded its browser extension to Safari, bringing real-time SaaS/AI monitoring, identity risk detection, and in-browser nudges to company Macs.

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

01 Safari browser extension for SaaS/AI visibility NEW

71

The Nudge Security extension now supports Safari, deployed silently to company Macs via Apple Business Manager and MDM. It monitors SaaS and AI activity in real time — including daily AI usage, logins, access patterns, and file uploads — and detects identity and access risks such as weak or reused passwords, SSO or MFA bypass attempts, shared credentials, and risky password manager use. It also delivers automated, customizable in-browser nudges to guide employees toward safer SaaS and AI behaviors.

Deploy the Nudge Security Safari extension silently to all company Macs so employees get SaaS/AI monitoring and nudges without any manual install step.

> 📍 In Nudge Security, go to Settings › Browser Extension › Safari and follow the step-by-step deployment instructions to push the extension via Apple Business Manager and your MDM.

— Names deployment path and specific risk/monitoring categories, but no config keys.

changelog-20260915-8c973857

WAS THIS USEFUL? 👍 👎

Ping Identity

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗

RANK

Read docs, explore use cases, learn best practices

> Ping Identity's PingOne AIC rapid channel release adds ESV-based configuration for connector server names with matching script-editor validation, alongside a batch of UI usability improvements to identity, job, and form management, plus a bulk connector version upgrade.

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

01 **ESV support for connector configuration and scripts** NEW

53

Connector configuration can now use an ESV (environment secret/variable) for the connector server name, and the script editor now shows errors when scripts reference environment ESVs incorrectly.

— Names the ESV mechanism and two surfaces but no exact field or key

changelog-20260915-040cebe6

02 **Streamlined identity, job, and modal management UI** IMPROVED

42

Admins can create another identity immediately after creating one without closing the modal, edit a scheduled job to start sooner than its originally configured future start time, close modals with the Escape key, and see forms clearly identify fields that contain errors after submission.

— Describes several UI behaviors but only general navigation, no exact paths

changelog-20260915-040cebe6

03 **Connectors upgraded to version 1.5.20.36** IMPROVED 28

All connectors have been upgraded to version 1.5.20.36.

— Bare version bump with no detail on changes or impact changelog-20260915-040cebe6

WAS THIS USEFUL? 👍 👎

iDenfy

Feedback ⓘ 1 RELEASE · SEEN 2026-09-15 NOTES ↗ RANK

Explore iDenfy documentation for identity verification (KYC), business verification (KYB), AML screening, fraud prevention, and more.

> iDenfy shipped automatic branding theme import from a website domain, a new `fields` filter parameter on the KYB company endpoint, native-script export columns in KYC CSV reports, and real-time framing feedback during document capture.

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

01 **`fields` parameter on KYB company endpoint** NEW 85

The KYB company endpoint now accepts a `fields` parameter to return only the requested data fields instead of the full response payload, reducing payload size.

Fetch only specific fields from the KYB company endpoint to reduce payload size and avoid processing unused data.

```
$ curl -X GET 'https://api.idenfy.com/api/v2/kyb/company?
fields=name,registrationNumber,status' \
  -H 'Authorization: Bearer <token>'
```

— Runnable curl example with exact endpoint and parameter values snapshot-20260915

02 **Auto-import branding from website domain** NEW 70

The verification UI theme can now be pre-filled automatically by pulling brand colors and logo from a website domain, eliminating manual palette setup. In the dashboard, go to Settings > IDV Flow & Branding, enter the website domain in the theme import field, and review the imported colors and logo before saving.

When onboarding a new client, pre-fill their verification UI theme automatically instead of entering colors manually.

> 📍 In the dashboard, go to Settings › IDV Flow & Branding, enter your website domain in the theme import field, and review the imported colors and logo before saving.

— Names exact UI path and steps, but no technical mechanism given snapshot-20260915

THINNER COVERAGE BELOW

03 **Native-script data columns in KYC CSV reports** NEW 45

KYC CSV reports gain an Original language data section that exports document field values in their native script as separate columns.

— Names the CSV section but no field names or column details snapshot-20260915

04 **Real-time framing feedback in document capture** IMPROVED 25

Document capture now provides real-time framing feedback during the capture flow.

— Single generic sentence, no mechanism or UI detail given snapshot-20260915

WAS THIS USEFUL? 👍 👎

◆ Secure Access (VPN / SASE / ZTNA)

Firezone

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

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

> Firezone's Windows client gains native support for ARM64 devices, shipping a dedicated installer alongside the existing x86-64 build.

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

01 **Native ARM64 Windows client installer** NEW 60

Firezone adds a native ARM64 (`aarch64`) installer for Windows on ARM devices, available alongside the existing x86-64 installer. WinGet automatically selects the correct installer for the detected CPU architecture.

— Names architecture and install mechanism but no version/commands

changelog-20260915-1bdf4685

WAS THIS USEFUL? 👍 👎

DNSFilter

Feedback ⓘ 1 RELEASE · 2026-09-15 CHANGELOG ↗ RANK

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

> DNSFilter's biggest update this window is the general availability of its MCP Server, letting AI assistants query DNS data and manage policies through natural language instead of the dashboard.

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

01 **DNSFilter MCP Server now generally available** NEW 83

The DNSFilter MCP Server integration is GA, letting AI assistants such as Claude, ChatGPT, and Codex query DNS activity and threat data, manage policies and allow/block lists, and automate reports and investigations via the Model Context Protocol without dashboard navigation. It's set up under Integrations → AI Connectors, where an admin opens the DNSFilter MCP Server card and copies the server URL to connect a client; the connection stays authorized for seven days before requiring reconnection.

Connect an AI assistant to DNSFilter so you can query DNS threat data and manage block lists in natural language, without touching the dashboard.

> 📍 In the DNSFilter console, go to Integrations → AI Connectors, open the DNSFilter MCP Server card, copy the server URL, then follow the MCP Server setup guide to point your client (Claude, ChatGPT, or Codex) at that URL.

— Names exact UI path, auth duration, and supported clients. changelog-20260915-cf1c67ab

WAS THIS USEFUL? 👍 👎

GOVERN

◆ AI/LLM Security

ai-safe2-framework

Feedback ⓘ 2 RELEASES · 2026-09-14

NOTES ↗ RANK

Ai-Safe2-Framework provides governance, risk, and compliance controls for securing agentic AI systems and non-human identities.

> AI SAFE² CLI shipped two new evidence-intake surfaces: a provider-neutral harness evidence command and a portable agent system identity manifest with strict validation, dual hashing, and schema export commands.

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

01 Portable agent system identity manifest and evidence commands

NEW 98

Adds `safe2 evidence system SOURCE --output FILE` to normalize an attributed agent-system identity declaration into a portable manifest, and `safe2 evidence manifest FILE --subject-id ID --output FILE` to bind that manifest into a wider hashed evidence run. A `--strict` flag on both `safe2 evidence system` and `safe2 evidence manifest` exits with status 1 when identity gaps, unknown evidence bases, missing versions, or disconnected components are detected. `safe2 schema export system-identity-source-v1` and `safe2 schema export system-identity-manifest-v1` export the provider-neutral input and normalized output contracts. The manifest models eight component categories (model, harness, tools, skills, memory, environment, policy, evaluator), a relationship graph of use, execution, policy, evaluation, memory, and delegation links, and an authority inventory of read, write, execute, network, delegate, approve, admin, or unknown classes per component. Dual hashing binds exact submitted bytes via `source.sha256` while `system_fingerprint_sha256` fingerprints normalized composition independent of key order, list order, and formatting; coverage recommendations surface remaining version, attribution, inventory, and topology gaps using four coverage statuses (complete, partial, missing, not-applicable) and three evidence-basis labels (observed, declared, unknown).

— Full command set, flags, and data model named with mechanism explained

2026-09-14_CLI_0.4.0_Know_What_You_Actu…

02 Provider-neutral harness evidence intake NEW 91

`safe2 evidence harness SOURCE --output FILE` validates and normalizes a provider-neutral harness export into a structured AI SAFE² evidence result. It assesses coverage across seven domains (task lifecycle, tool calls, artifacts, tests, usage, environment state, and completion claims), records a SHA-256 digest and size binding the exact export processed, preserves evidence attribution (producer, export identifier,

source references, and collection basis), and produces loss-aware recommendations that surface which evidence areas remain partial or missing rather than treating gaps as success. It establishes a stable integration seam targeting Codex, Claude Code, Hermes, OpenClaw, and other agent harnesses.

— Named command and concrete mechanism, but no usage example given

2026-09-14_CLI_0.3.0_Provider_Neutral_H…

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · September 15, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe | Feedback on this issue