THE CYBER TOOLCHAIN

NO. 127

# Tail

THE DAILY RELEASE FIREHOSE

PUBLISHED NOVEMBER 1, 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 80 changes

Do you prefer **scroll**? 👍 👎

▸ // CONTENTS SHOW 25 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. Aikido Security now walks an external perimeter from one domain and chains CVEs and exposed secrets into ing exploit paths, no pentest engagement needed. FOSSA runs

vim ? help

impact analysis on dependency-bump PRs before merge, so upgrades stop breaking builds. Salt Security lets API threat workflows revoke and block on their own instead of filing a ticket.

PROTECT

**See your internet-facing attack surface the way an attacker chains it, from one domain**

Aikido's agents enumerate the perimeter, attack what they find with known CVEs, misconfigurations and exposed secrets, and join findings into full exploit paths — the chaining is the part a vulnerability list never gives you. Censys's move to flat one-credit search, daily free searches and credit rollover makes exploratory external recon something you do on a hunch rather than budget against.

Aikido Security · Censys

PROTECT

**Stop a dependency upgrade from breaking the build before you merge it**

FOSSA's fossabot runs application impact analysis on upgrade PRs — including PRs raised by existing auto-PR bots — so the merge decision carries evidence instead of hope, which is the main reason dependency bots get muted. Mend SCA now parses both Bun lockfile formats with reachability and workspace support, closing a blind spot for teams that moved off npm; Endor Labs packages a fully automated SCA Remediation agent grounded in its own reachability and policy data.

FOSSA · Mend SCA · Endor Labs

RESPOND

**Let an API threat workflow contain itself instead of paging someone**

Autonomous Defense gives Salt Workflows the authority to block, revoke and remediate against connected controls directly, with a visual builder and 200+ prebuilt connectors to reach gateways and IdPs. The gap it closes is the one between Salt detecting a live API abuse and a human logging into another console to shut off the key.

Salt Security

## OFFENSIVE SECURITY

◆ Reconnaissance & OSINT

## Hunter

Feedback ⓘ announced · Oct 29, 2026 BLOG ↗ RANK

Hunter is a contact anyone. Unlock opportunities.

> Hunter launched an official MCP server, letting AI assistants call its contact-finding, verification and CRM tools directly, with one-click OAuth setup on every plan including Free.

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

01 **Official MCP server for AI assistants** NEW 86

Hunter now offers an MCP server at `https://mcp.hunter.io/mcp`, exposing over 100 tools covering email finding, verification, enrichment, sequences, saved searches, company lists, and CRM sync to any MCP-compatible AI client. It works with Claude, ChatGPT, Gemini, Perplexity, Claude Code, Cursor, Codex, and other MCP-compatible clients, and is included on every Hunter plan including Free. Connection uses a one-click OAuth flow that passes the Hunter API key in an `X-API-Key` header, so no manual API key configuration is required.

Register the Hunter MCP server in a Claude or compatible client config so your AI assistant can call Hunter tools directly.

json

```
{
  "mcpServers": {
    "hunter": {
      "url": "https://mcp.hunter.io/mcp"
    }
  }
}
```

— Names endpoint, auth header, client list and gives config example

launch-20261029-2c559235

└──▷ **ALSO FROM THESE RELEASES**

WAS THIS USEFUL? 👍 👎

## APPLICATION SECURITY

◆ Web Application Security

# humble

Feedback ⓘ 1.68 NOTES ↗ RANK

A humble and fast security-oriented HTTP headers analyzer.

> humble 1.68 adds Markdown export, a version-lag check for the CLI, and 16 new insecure header detections.

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

01 **Markdown export format for analysis results** NEW 60

Analysis results can now be exported to Markdown using `-o md`.

— Names exact flag but no further mechanism detail 1.68

02 **Version lag check via -v flag** NEW 60

Running `-v` now shows how many days behind the latest release the installed version of humble is, e.g. `python humble.py -v`.



Check whether your installed copy of humble is behind the latest release and by how many days.

```
$ python humble.py -v
```

— Exact flag and runnable example given, mechanism simple 1.68

THINNER COVERAGE BELOW

03 **16 new insecure header checks** NEW 25

Adds 16 new insecure header checks across multiple categories.

— No specific header names or categories listed 1.68

WAS THIS USEFUL? 👍 👎

◆ SAST / SCA / Code Security

## skylos Feedback ⓘ v5.3.0 NOTES ↗ RANK

Open source local-first PR scanner that finds dead code, security bugs, secrets, quality regressions, and AI-code mistakes before merge. For first timers refer to https://duriantaco.github.io/skylos/repo-map/

> Skylos v5.3.0 adds an opt-in AI review step that runs automatically when scan results are uploaded for the default branch.

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

01 **AI review on default-branch cloud uploads** NEW 50

Running `skylos cloud` to upload results for the default branch now triggers an AI review step as part of that process.

— Names the exact command but not what the AI review checks or outputs v5.3.0

WAS THIS USEFUL? 👍 👎

## Mend.io Mend SCA

Feedback ⓘ announced · Oct 29, 2026 BLOG ↗

RANK

Mend sca is a traditional application security misses AI risk. Standalone AI security tools miss your code.

> Mend SCA adds full support for Bun-managed JavaScript and TypeScript projects, including both lockfile formats, reachability analysis, workspaces and private registries.

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

01 **Bun project scanning with reachability analysis** NEW

77

Mend SCA now scans Bun-managed JavaScript and TypeScript projects by reading `bun.lock` (the text format, default since Bun 1.2) with no Bun installation required in the scan environment, and also supports the legacy binary `bun.lockb` format when Bun is installed in the scan environment. Reachability analysis is supported for Bun projects in the Mend CLI and all repository integrations, marking each dependency vulnerability as reachable or unreachable for both JavaScript and TypeScript sources. Bun workspaces and private registries are supported with no extra configuration, and any folder containing a `package.json` alongside a `bun.lock` or `bun.lockb` file is automatically detected and scanned as a Bun project.

— Names exact lockfiles and mechanism but no CLI command given launch-20261029-7e79d4f1

WAS THIS USEFUL? 👍 👎

## FOSSA

Feedback ⓘ announced · Oct 29, 2026 BLOG ↗ RANK

FOSSA secures the software supply chain with automated SBOM generation, software composition analysis, license compliance, and vulnerability management.

> FOSSA launched Context-Aware Remediation, a fossabot-powered workflow that runs application impact analysis on dependency-upgrade PRs before merge, extending to existing auto-PR tools and multiple language ecosystems.

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

### 01 Context-Aware Remediation for dependency upgrade PRs NEW

80

Clicking `Create PR` on a security issue in FOSSA opens a pull request and runs an application impact analysis drawing on your test suites, interfaces, and CI signals, powered by fossabot. The same breaking-change analysis now also runs on PRs opened by Dependabot, Renovate, or Snyk, making those existing auto-PR workflows context-aware without replacing them. It supports JS/TS, Python, and Java ecosystems via Quick Import from GitHub, with additional ecosystems planned. If a build fails after an upgrade, commenting `@fossabot fix` on the PR has fossabot read the CI failure output, generate a fix, and commit it to the PR branch.

When a security issue appears in FOSSA and the upgrade breaks the build, comment directly on the PR to have fossabot diagnose the CI failure and push a corrective commit.

> 📍 Steps: 1. Open the pull request that fossabot created for the security issue. 2. Review the impact-analysis comment fossabot posted, which lists what it checked. 3. If the build is red, comment `@fossabot fix` on the PR. 4. fossabot reads the CI failure output, generates a fix, and commits it to the PR branch.

— Explains mechanism and exact trigger comment, but limited ecosystem/numeric detail

launch-20261029-fcd14dea

WAS THIS USEFUL? 👍 👎

# Aikido Security

Feedback ⓘ announced · Oct 28, 2026 BLOG ↗

RANK

Aikido Security is a developer-focused application security platform that scans code, dependencies, containers, and cloud infrastructure to detect and help fix vulnerabilities.

> Aikido Security launched external network pentesting, where AI agents map an organization's entire internet-facing perimeter from a single domain, attack discovered hosts using known CVEs, misconfigurations and exposed secrets, and chain findings into full exploit paths.

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

## 01 External network pentesting from a single domain NEW

78

Aikido now runs external network pentests starting from a single domain, where AI agents discover subdomains and internet-facing hosts — websites, APIs, VPN gateways, mail servers, self-hosted tools — and attack each one using known CVEs, misconfigurations, and exposed secrets. Launched via Pentesting > External Network, where you enter a root domain, verify ownership, review the auto-generated asset list, and confirm a quote before agents begin mapping and attacking discovered hosts.

Start an external network pentest when you want to see everything attackers can reach under your domain before they do.

> 📍 In the Aikido product, go to Pentesting › External Network, enter your root domain, verify ownership, review the auto-generated asset list (remove any hosts you do not want tested), confirm the quote, and launch the pentest. Agents begin mapping subdomains and attacking each discovered host immediately.

— Names mechanism, asset types, and exact UI navigation path launch-20261028-dec412a3

THINNER COVERAGE BELOW

## 02 Fix suggestions with retest agent NEW

57

Each finding includes a fix suggestion and a retest agent that checks whether the fix resolved the issue and whether it opened a new weakness elsewhere; retests are available for up to six months.

— Named limit (six months) but no interface detail launch-20261028-dec412a3

## 03 Multi-step exploit chaining across findings NEW

56

Agents chain multi-step findings — for example, an exposed `.git` folder leading to SSH credentials leading to Azure admin access — and include the full exploit chain in the report so teams can see what an attacker could actually reach.

— Concrete example chain but no action a reader takes launch-20261028-dec412a3

04 **Continuous external perimeter pentesting mode** NEW

44

A continuous pentesting mode re-maps the perimeter on every run and starts testing newly discovered hosts shortly after they go live, rather than waiting for a scheduled engagement.

— Explains behaviour but no configuration detail given launch-20261028-dec412a3

05 **Unified pentest platform and audit-ready reporting** IMPROVED

37

External network pentesting runs inside the same product as Aikido's existing web app and mobile pentests, with a shared findings and retest interface and the same proof-of-exploit standard across all pentest types. Every pentest produces an audit-ready report with validated findings, proof of exploit, and remediation guidance suitable for compliance and auditor review.

— Describes integration and report contents only in prose launch-20261028-dec412a3

WAS THIS USEFUL? 👍 👎

◆ Software Supply Chain Security

# Endor Labs

Feedback ⓘ announced · Oct 29, 2026 BLOG ↗ RANK

Endor Labs is an application security platform built for AI-generated and human-written code, helping teams prioritize and fix real risk across the SDLC.

> Endor Labs shipped a one-click plugin that brings its MCP server into Google Antigravity, plus a suite of pre-built AURI Agents — including a fully automated SCA Remediation agent — that let teams hand security backlog work off to agents grounded in Endor Labs' reachability and policy data.

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

## 01 One-click Endor Labs plugin for Google Antigravity NEW

65

Endor Labs ships a one-click plugin in the Google Antigravity marketplace that installs the Endor Labs MCP server inside Antigravity, letting agents check packages for vulnerabilities, malware, or exposed secrets before a pull request is opened. After installing the plugin, a user can prompt the Antigravity agent to scan the project, check dependencies, and flag exposed secrets.

Trigger a full security review of your project inside an Antigravity session immediately after installing the plugin.

> 📍 Install the Endor Labs plugin from the Plugin marketplace in Antigravity, then prompt the Antigravity agent: 'Scan my project for security flaws, check all dependencies for vulnerabilities or malware, and flag any exposed secrets.'

— Names the marketplace and MCP server with an install-and-prompt example.

launch-20261029-a71d5f2e

THINNER COVERAGE BELOW

## 02 AURI Agents available inside Antigravity NEW

46

Four pre-built AURI Agents — SCA Remediation, AI SAST Triage, Dependency Decision Helper, and Vulnerability Explainer — are now available inside Antigravity, letting teams hand off backlog security work to agents grounded in Endor Labs reachability, upgrade-impact, findings, and policy data.

— Names all four agents but gives no individual mechanism for three of them.

launch-20261029-a71d5f2e

WAS THIS USEFUL? 👍 👎

◆ WAF, Bot & API Protection

## Salt Security

Feedback ⓘ announced · Oct 28, 2026 BLOG ↗

RANK

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

> Salt Security launched Autonomous Defense, letting Salt Workflows automatically block, revoke, and remediate active threats across connected controls, alongside a new visual workflow builder with 200+ prebuilt connectors.

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

### 01 Autonomous Defense actions via Salt Workflows NEW

70

Salt Workflows can now trigger automated remediation when Salt detects risk: blocking active attacks at connected WAFs, API gateways, and other enforcement points during exploitation; revoking agent and MCP tool access by disabling unauthorized MCP connections, quarantining shadow tools, or removing excess privilege; and enforcing AI and data protections at runtime by updating connected guardrail policies, blocking unsafe AI requests, or redacting sensitive data through connected gateways.

– Mechanisms named for each action but no exact config or API surface

launch-20261028-f4bcf534

### 02 Drag-and-drop workflow builder with 200+ connectors NEW

60

Salt adds a visual drag-and-drop workflow builder directly into the Agentic Security Platform, shipping with 200+ out-of-the-box connectors and a marketplace of integrations spanning security, infrastructure, IT, and collaboration systems.

– Connector count and scope named, but no exact UI path or API launch-20261028-f4bcf534

WAS THIS USEFUL? 👍 👎

## CLOUD & CONTAINER SECURITY

◆ Cloud Security Posture

## Lacework FortiCNAPP

Feedback ⓘ changelog · Nov 1, 2026

CHANGELOG ↗

Lacework FortiCNAPP is a cloud-native application protection platform from Fortinet that secures cloud workloads, containers, and infrastructure through vulnerability scanning, misconfiguration detection, and runtime threat monitoring.

Lacework FortiCNAPP's intrusion graph now shows why entities in a composite alert are connected; Linux Agent 8.5.0 released October 22, 2026.

Lacework FortiCNAPP's intrusion graph now shows why entities in a composite alert are connected.

Linux Agent 8.5.0 is now available (released October 22, 2026).

NEW SUPPORTED PLATFORM Vulnerability assessment for Microsoft Azure Linux (CBL-Mariner)

WAS THIS USEFUL? 👍 👎

◆ CNAPP

## Plerion

Feedback ⓘ Top risks now cover Azure and GCP storage:

NOTES ↗

Plerion is a cloud security platform that detects misconfigurations, vulnerabilities, and threats across cloud environments and provides remediation guidance.

NEW DETECTION Publicly readable Azure blob container and Google Cloud Storage bucket top-risk detection

WAS THIS USEFUL? 👍 👎

# DETECTION & RESPONSE

◆ SIEM

# Databricks

Feedback ⓘ

Managed warehouse for MLflow (Beta) (2026-11-02) BLOG ↗ RANK

Databricks is a cloud-based data lakehouse platform for data engineering, analytics, machine learning, and AI workloads, built on Apache Spark.

> Databricks introduced a Beta managed warehouse for MLflow traces, removing the need to manually select a SQL warehouse to view Unity Catalog traces.

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

01 **Managed warehouse for MLflow traces (Beta)** NEW 65

Enabling Managed Warehouse for MLflow on the Previews page lets users query Unity Catalog traces in the MLflow UI without manually selecting a SQL warehouse; MLflow automatically provisions its own warehouse or falls back to serverless compute.

Workspace admins enabling managed warehouse so analysts can view MLflow traces without configuring a SQL warehouse

📍 In the Databricks console, go to Settings › Previews and enable Managed Warehouse for MLflow.

— Names exact UI path and behavior but lacks limits or scope detail.

Managed warehouse for MLflow (Beta) (20…

WAS THIS USEFUL? 👍 👎

◆ Endpoint Security (EDR/XDR)

# Trend Vision One

Feedback ⓘ

File Security Storage template version 2.5.0 for Google Cloud (2026-11-02)

BLOG ↗ RANK

Trend Vision One is Trend Micro's unified cybersecurity platform that consolidates threat detection, response, and risk management across endpoints, cloud, email, and networks.

> Trend Vision One's File Security Storage Google Cloud template (v2.5.0) adds scanning of dual- and multi-region Cloud Storage buckets, location-specific destination buckets, configurable Cloud Run scaling, and failure reporting for scans that exceed the retry limit.

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

01 **Cloud Run scaling and CPU allocation for scan services** NEW

75

The Google Cloud template lets you configure Cloud Run scaling and CPU allocation for the Scanner and Post-Scan Action services, with scale-to-zero and request-based billing enabled by default.

– Names the two services and default billing/scaling behaviour.

File Security Storage template version …

02 **Dual-region and multi-region bucket scanning** NEW 60

File Security Storage can now scan dual-region and multi-region Cloud Storage buckets in the Google Cloud template, provided the File Security Storage service has a matching update and a scanner is deployed in an eligible region.

– Names requirement (matching service update, eligible-region scanner) but no exact config path.

File Security Storage template version …

THINNER COVERAGE BELOW

03 **Location-specific destination buckets for scan results** NEW

50

The Google Cloud template now supports configuring separate, location-specific destination buckets for clean, malicious, and failed files.

– States the three bucket categories but no config key or UI path.

File Security Storage template version …

04 **Failure reports for scan requests exceeding retry limit** NEW

File Security Storage now generates failure reports for scan requests that exceed the retry limit.

— Thin description with no mechanism or configuration detail.

File Security Storage template version …

WAS THIS USEFUL? 👍 👎

## SentinelOne

Feedback ⓘ announced · Oct 30, 2026 PRESS ↗ RANK

SentinelOne's Singularity platform protects endpoints, cloud, identity and data with AI-driven detection, Purple AI and an agentic SOC layer.

> SentinelOne shipped Singularity Agentic Detection and Response to discover, monitor and contain AI agents across the enterprise, and added Anthropic's Claude Mythos 5.1 model to its Wayfinder Frontier AI Services for exploitability-validated vulnerability assessment.

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

01 **Agentic Detection and Response for AI agents** NEW 75

Singularity Agentic Detection and Response (ADR) builds an inventory of AI agents, tools, connectors, and Model Context Protocol (MCP) servers along with their permissions and associated users, supporting agents built on Salesforce Agentforce, Microsoft Copilot Studio, OpenAI ChatGPT workspace agents, and Anthropic Claude managed agents. It monitors agent activity through event traces that link AI-driven actions to subsequent system processes to detect deviation from an agent's assigned task, and it detects and blocks threats including prompt injection and credential exfiltration before agent actions execute. Security teams can set controls governing which agents are allowed to operate and which resources they can access, contain an individual agent without stopping the wider workflow, and agent activity is integrated into the Singularity Platform's existing investigation and response workflows so teams can examine agent actions and automate responses within customer-defined boundaries.

– Clear mechanism and named integrations but no exact UI path or API given

launch-20261030-2d04f863

THINNER COVERAGE BELOW

02 **Claude Mythos 5.1 added to Wayfinder Frontier AI Services**

NEW 48

Wayfinder Frontier AI Services now includes Anthropic Claude Mythos 5.1, a restricted-access model, alongside existing OpenAI and Anthropic models to improve vulnerability discovery and exploitability confirmation. Findings are filtered through exploitability testing so customers receive validated results and prioritised remediation guidance rather than raw vulnerability lists.

– Names the model and testing mechanism but no config or API surface

launch-20261030-e5b68b0c

WAS THIS USEFUL? 👍 👎

◆ Threat Intelligence

## Cloudmersive

Feedback ⓘ changelog · Nov 1, 2026 CHANGELOG ↗

RANK

Cloudmersive is a developer API platform offering cloud-based services for file scanning and malware detection, document conversion, image processing, and data validation.

> Cloudmersive's Cloud Virus API gained additional custom policy features in version v11-11-11.

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

### 01 Custom policy features in Cloud Virus API IMPROVED

35

Cloud Virus API `v11-11-11` now supports additional custom policy features, though the specific policies added are not detailed.

— Names API and version but no specific policy details changelog-20261101-8b5fe42e

WAS THIS USEFUL? 👍 👎

## EXPOSURE & VULNERABILITY MANAGEMENT

◆ Endpoint Management (UEM/RMM)

# Iru

Feedback ⓘ changelog · Nov 1, 2026 CHANGELOG ↗ RANK

Iru is a device-centric platform that unifies security, IT, and compliance around devices and everything they touch.

> Iru shipped Remote Shell for macOS detections, letting admins open a terminal to a managed Mac even under partial isolation, and expanded its Windows Auto App catalog with six new applications.

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

01 **Remote Shell for managed Macs in EDR** NEW 76

A Launch Remote Shell button inside the detection window opens a secure terminal tunnel to a managed Mac without leaving the investigation context. The connection stays alive through partial device isolation, so containment and investigation can happen simultaneously, and Remote Shell is also available as an add-on for customers running Iru Endpoint Management without the EDR package.

Contain a suspicious Mac and investigate without losing detection context or pivoting between tabs.

> 📍 In the Iru console, open the firing detection, apply partial isolation to the device, then click Launch Remote Shell to open a terminal beside the detection details and device posture — the shell stays reachable even while the device is isolated.

— Clear mechanism and UI path, but no CLI/API surface named. launch-20261028-ba653c2c

THINNER COVERAGE BELOW

02 **Six new Windows Auto Apps added to catalog** NEW 40

Iru adds six new Windows Auto Apps: Make Me Admin, Meld, Microsoft PowerBI Desktop, Netbird, PDF-XChange Editor, and Private Internet Access.

— Names all six apps but no mechanism or usage detail. changelog-20261101-09b67ef2

WAS THIS USEFUL? 👍 👎

◆ Attack Surface & Exposure Management

# Censys

Feedback ⓘ announced · Oct 30, 2026 BLOG ↗ RANK

Censys is a internet-wide scanning and search platform that discovers and monitors hosts, services, and certificates to help security teams assess their exposure.

> Censys overhauled its pricing model with flat one-credit search pricing, new Starter subscription tiers, daily free searches for all users, and credit rollover.

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

01 **Starter and Starter Pro subscription tiers** NEW 70

Censys adds a Starter plan at $79/month with 500 credits, 2 Collections, and 10 asset tags, and a Starter Pro plan at $599/month with 4,000 credits, 4 Collections, and 25 asset tags.

– Concrete prices and limits for both new plans, but no signup flow detail.

launch-20261030-2157fb23

02 **Flat one-credit pricing for all search actions** IMPROVED 65

Censys now prices every search action — lookups, standard searches, and advanced regex queries — at one credit each, replacing the previous 1/5/8-credit tiered model.

– Clear before/after and named query types, but no exact dates. launch-20261030-2157fb23

THINNER COVERAGE BELOW

03 **Five free daily searches for registered users** NEW 45

Every registered Censys user now gets five free searches per day that do not draw from subscription credits.

– States the mechanism and number but no further detail. launch-20261030-2157fb23

04 **Monthly credit rollover** NEW 35

Unused monthly subscription credits now roll over into the next billing cycle instead of expiring.

– Simple behavior change with no limits or mechanism specified. launch-20261030-2157fb23

WAS THIS USEFUL? 👍 👎

◆ Identity & Access Management

# Clerk

Feedback ⓘ changelog · Nov 1, 2026 CHANGELOG ↗ RANK

Clerk is an authentication and user-management platform that provides pre-built UI components, APIs, and SDKs for adding sign-up, sign-in, and identity features to applications.

> Clerk's biggest addition this window is passkeys as a full second MFA factor, alongside a new Backend API logs endpoint, an MCP-based agent feedback tool, Clerk Protect rules against bulk sign-ups, and an early-beta Agent Auth offering — plus a breaking change to test-mode email delivery.

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

01 **Backend API audit logs endpoint** NEW 85

Query audit logs programmatically with the `GET /v1/logs` Backend API endpoint, filtering on the same event types available in the Dashboard. Requests over the rate limit return `too_many_requests`.

— Names exact endpoint, filters, and error code. changelog-20261101-d5b03bac

02 **Agent feedback collection via MCP** NEW 65

Collect agent feedback through your MCP server by adding the `submit_feedback` tool from `@clerk/mcp-tools`, so agents can report friction — missing tools, unexpected errors, or blocked tasks — as they encounter it.

— Names package and tool but lacks setup detail. changelog-20261101-d5b03bac

03 **Bulk sign-up protection rules in Clerk Protect** NEW 60

Two new Clerk Protect rules limit bulk account creation on the Business plan: Limit sign-ups per email domain caps sign-ups from one domain per hour, and Limit sign-ups from shared infrastructure caps bursts from the same infrastructure.

— Names both rules but not the exact toggle location. changelog-20261101-d5b03bac

04 **Test-mode emails stop reaching +clerk_test addresses** BREAKING 60

Test email addresses using the `+clerk_test` subaddress no longer receive any emails while Test mode is on. Test suites that read sign-in links or invitation emails from a real inbox must switch those addresses to ones without `+clerk_test`.

— Clear before/after with a migration instruction. changelog-20261101-d5b03bac

THINNER COVERAGE BELOW

05 **Clerk for Agent Auth private beta** NEW 45

Clerk for Agent Auth, built on open OAuth standards and the Personal Agent Protocol, is now in private beta, enabling agents to discover your application and authenticate through Clerk.

— Beta announcement with no setup steps yet. changelog-20261101-d5b03bac

└──▷ **BREAKING ON UPGRADE**

! Test email addresses ( `+clerk_test` subaddress) no longer receive any emails while Test mode is on — test suites that read sign-in links or invitation emails from a real inbox must switch those addresses to ones without `+clerk_test` .

---

WAS THIS USEFUL?  

## ConductorOne

Feedback ⓘ October 30, 2026 (2026-10-31) BLOG ↗

RANK

ConductorOne is an identity governance platform that automates workforce access management and deploys AI agents to streamline access reviews and provisioning.

> ConductorOne shipped Role Mining Suggestions for surfacing group-based access profiles, expanded MCP gateway visibility and admin controls, richer access-review campaign filtering and C1 group management, plus a wide set of breaking API, logging, and permission changes including a 16-rule policy limit and removal of the `email capabilities` gRPC method.

└──▷ **WHAT SHIPPED · 16 FEATURES** most completely described first ? what's the number?

### 01 Compliance framework and app annotation approval routing NEW

80

Policies, approver steps, entitlement routing rules, account provisioning, and forms can now check compliance frameworks and app annotations to route approvals — for example, routing SOX-tagged access requests through a dedicated approval step via a Compliance framework condition in the policy editor.

Route SOX-tagged access requests through a dedicated approval step using the new compliance framework condition in a policy.

> 📍 In the Policy editor, add an approver step, open its conditions, select Compliance framework as the attribute, choose SOX, and assign the dedicated SOX approver group.

— Concrete example walks through exact policy editor steps October 30, 2026 (2026-10-31)

### 02 MCP gateway visibility and error reporting IMPROVED

75

AI agents connected through the MCP gateway now see every MCP server available to them, with access status and toolsets listed per server. MCP gateway error responses report whether a rejected token expired, was revoked, or is malformed, returning error code `-32010` when a server credential requires reauthorization.

— Exact error code and failure types named, no remediation command

October 30, 2026 (2026-10-31)

### 03 invalid_client replaces invalid_grant for failed token requests

75

BREAKING

Failed client credentials token requests now always return `invalid_client` instead of a specific reason — scripts or SIEMs matching on `invalid_grant` to detect deleted, disabled, or expired credentials must match `invalid_client` instead.

— Exact old and new error codes given for migration October 30, 2026 (2026-10-31)

---

04 **email capabilities gRPC method removed** BREAKING 75

The `email capabilities` gRPC method on the provider service is removed — clients must move to the capabilities service ( `GET /api/v1/settings/email-capabilities` is unchanged).

— Exact gRPC method and replacement REST endpoint named October 30, 2026 (2026-10-31)

---

05 **Campaign filtering and entitlement exclusion controls**

IMPROVED 70

Access review campaigns can now be filtered using custom selectors on resource attributes and entitlement annotations, combinable with app, resource type, risk level, and compliance framework filters, and grant usage filters can be set to Used in the last [timeframe] or Unused in the last [timeframe] . Admins can also exclude specific entitlements, or everything matching a custom selector, from campaigns and templates.

— Names filter mechanics and values but gives no exact UI path

October 30, 2026 (2026-10-31)

---

06 **MCP server tool access presets and manual connection** NEW

70

Admins can assign automatic tool access per MCP server by choosing a preset ( Read tools , All tools ) or creating a named toolset, and can connect external MCP servers manually by selecting Configure manually to supply custom OAuth client credentials or use a public client.

— Names exact preset labels and manual-connection option October 30, 2026 (2026-10-31)

---

07 **C1 groups membership review and creation** NEW 65

C1 groups, including automated groups, can now be reviewed for membership inside access review campaigns, and admins can create a C1 group from an existing group or entitlement, with C1 proposing a membership rule, inclusion and exclusion lists, and flagging anyone who cannot be adopted.

— Explains mechanism of proposal and flagging, no exact UI steps

October 30, 2026 (2026-10-31)

---

08 **Resource descriptions from source systems** IMPROVED

65

Turning on `Use resource descriptions` in an app's Entitlement management settings shows source-system descriptions instead of connector-generated text.

— Exact setting name and location given `October 30, 2026 (2026-10-31)`

09 **System log and MCP denial logging accuracy** `BREAKING`

65

System log entries for failed token requests now record the real failure reason, and MCP tool calls refused by authorization are recorded as `denied` instead of a generic failure with code 500 — SIEM rules or alerts matching the old status details must be updated.

— Specific before/after status detail given `October 30, 2026 (2026-10-31)`

10 **Slack /c1 shortcut for access requests** `NEW` 60

Typing `/c1` in Slack now opens the access request form directly, equivalent to `/c1 request`.

Quickly open an access request in Slack without switching to the browser.

```
$ /c1
```

— Runnable slash command given verbatim `October 30, 2026 (2026-10-31)`

11 **Remediate with AI for unowned NHI findings** `NEW` 60

Admins can get AI-suggested owners for unowned non-human identity findings via `Remediate with AI`, which shows up to three candidates with confidence levels.

— Names feature and output but no exact invocation path `October 30, 2026 (2026-10-31)`

12 **Administrative permission tightening** `BREAKING` 60

Application Administrators who do not own an app can no longer change an entitlement's owners, automations, or manual membership unless they are also Super Administrators; Basic Users can no longer list or download app population reports; and only Super Administrators and Read-Only Administrators can read email provider settings and email activity.

— Names exact roles and restricted actions, no endpoint given `October 30, 2026 (2026-10-31)`

THINNER COVERAGE BELOW

13 **New request sidebar button** `NEW` 55

Users can start an access request from anywhere in ConductorOne using the new sidebar `New request` button, which opens a right-side panel without leaving the current view.

— Names exact UI control and its behavior October 30, 2026 (2026-10-31)

---

14 **Deleted service principal credential API behavior change** 55

BREAKING

Reading, updating, or creating a credential for a deleted service principal now returns `not found` instead of succeeding — scripts or Terraform relying on the old behavior must be updated.

— Clear before/after but no exact endpoint path named October 30, 2026 (2026-10-31)

---

15 **Policy conditional rule limit** BREAKING 55

Policies are now limited to 16 conditional rules — existing policies above the limit remain editable but cannot grow beyond their current size.

— Exact numeric limit given, no migration path beyond note October 30, 2026 (2026-10-31)

---

16 **Personal API key field update validation** BREAKING 50

Updating a personal API key's roles or allowed source IPs through the API now returns an error for fields that cannot be changed, instead of silently ignoring them.

— Names affected fields but no endpoint path October 30, 2026 (2026-10-31)

## └──▷ ALSO FROM THESE RELEASES

## └──▷ BREAKING ON UPGRADE

! Failed client credentials token requests now always return `invalid_client` instead of a specific reason — scripts or SIEMs matching on `invalid_grant` to detect deleted, disabled, or expired credentials must match `invalid_client` instead.

! Reading, updating, or creating a credential for a deleted service principal now returns `not found` instead of succeeding — update any scripts or Terraform that relied on the old behavior.

! Updating a personal API key's roles or allowed source IPs through the API now returns an error for fields that cannot be changed, instead of silently ignoring them.

! System log entries for failed token requests now record the real failure reason, and MCP tool calls refused by authorization are recorded as `denied` instead of a generic failure with code 500 — update SIEM rules or alerts that matched the old status details.

! The `email capabilities` gRPC method on the provider service is removed — clients must move to the capabilities service ( `GET /api/v1/settings/email-capabilities` is unchanged).

- ! Application Administrators who do not own an app can no longer change an entitlement's owners, automations, or manual membership unless they are also Super Administrators; Basic Users can no longer list or download app population reports; only Super Administrators and Read-Only Administrators can read email provider settings and email activity.
- ! Policies are now limited to 16 conditional rules — existing policies above the limit remain editable but cannot grow beyond their current size.

---

WAS THIS USEFUL?  

◆ Secure Access (VPN / SASE / ZTNA)

# Zscaler

Feedback ⓘ changelog · Oct 30, 2026 BLOG ↗ RANK

Zscaler is a cloud-based security platform that protects users and data by routing internet and private application traffic through policy-enforced zero trust gateways.

> Zscaler's October 2026 GovCloud update brings Real User Monitoring to ZDX, ships Client Connector 5.0 for Windows with new network, TLS, resiliency and DLP capabilities, adds appliance terminal access to Zero Trust Branch, and extends Cloud Connector with AWS account tagging and VDI provisioning roles.

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

01 **Client Connector 5.0 for Windows feature set** NEW 80

Client Connector 5.0 for Windows adds Wi-Fi Name (SSID) as a trusted network criterion, TLS 1.3 support with automatic fallback to TLS 1.2, and machine tunnels in Business Continuity mode to keep devices connected to Private Access apps when the Zscaler cloud is unreachable (requires Windows 11 24H2 build 26100 or later; Limited Availability). It also adds Endpoint DLP on ARM-based Windows machines (requires ZDP Module 26.08 or later).

— Names exact requirements and versions but no config path 2026-10-30-146f5364

02 **AWS account tagging and VDI provisioning roles in Cloud Connector**

NEW 71

Cloud Connector now supports AWS account tagging across cross-account deployments with workload communications for multi-account environment organization (FedRAMP Moderate; Limited Availability), and adds a VDI Provisioning permission when adding admin roles, with Full, View Only, or None options for role-based access control over virtual desktop infrastructure (FedRAMP Moderate and High).

— Names two concrete additions and their option values 2026-10-30-146f5364

THINNER COVERAGE BELOW

03 **Appliance Admin Console in Zero Trust Branch** NEW 55

Zero Trust Branch 8.2.1-P1 adds an Appliance Admin Console page giving administrators terminal access to appliances for troubleshooting (FedRAMP Moderate and High; Limited Availability).

— Names the console page as a clear starting point 2026-10-30-146f5364

04 **Real User Monitoring in ZDX** NEW 47

Zscaler Digital Experience (ZDX) now includes Real User Monitoring, capturing and analyzing browser-level user interactions with applications to give visibility into performance bottlenecks (FedRAMP Moderate).

— Describes purpose but no UI path or metrics given 2026-10-30-146f5364

---

05 **Windows 32-bit support dropped in Client Connector 5.0**

30

BREAKING

Zscaler Client Connector 5.0 for Windows does not support Windows 32-bit.

— Bare statement with no migration guidance 2026-10-30-146f5364

└──▷ **BREAKING ON UPGRADE**

! Zscaler Client Connector 5.0 for Windows does not support Windows 32-bit.

---

WAS THIS USEFUL? 👍 👎

# Zscaler Internet Access

Feedback ⓘ

changelog · Oct 30, 2026 | BLOG ↗ | RANK

Zscaler Internet Access is a cloud-based secure web gateway that routes user traffic through a zero-trust proxy to enforce security policies, block threats, and control access to the internet and SaaS applications.

> This release centers on Endpoint DLP 26.08, broadening device control, indexing and OCR capabilities, and adds new Zoom AI transcript scanning that requires existing tenants to reauthorize their integration.

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

## 01 Zoom AI transcript and meeting summary scanning

BREAKING

65

Zoom tenants using Data at Rest Scanning DLP and Malware can now scan AI transcripts and AI meeting summaries generated by Zoom AI Companion. Existing Zoom tenants onboarding this capability must add additional scopes, webhook subscriptions, and reauthorize their Zoom integration.

— Names required reauthorization steps, actionable for admins 2026-10-30-f0dbe129

THINNER COVERAGE BELOW

## 02 Device Control extended to portable devices and removable media

NEW

55

Endpoint DLP 26.08 now extends Device Control to portable devices (smartphones and cameras), CD/DVD, and floppy disk channels (floppy disk is Windows only).

— Names exact device channels but no policy config details 2026-10-30-f0dbe129

## 03 IDM indexing removes 20-file folder limit

IMPROVED

50

Endpoint DLP 26.08 now lets IDM index all files in a folder, removing the previous 20-file limit.

— Gives clear before/after but lacks config specifics 2026-10-30-f0dbe129

## 04 Real-time OCR support for PDFs

NEW

50

Endpoint DLP 26.08 adds real-time OCR support for PDFs across all channels except Application File Access.

— Scope of channels named, no mechanism detail 2026-10-30-f0dbe129

05 **CSV export for Application Inventory** NEW — 35

Endpoint DLP 26.08 adds a CSV export for Application Inventory.

— Names format and feature but no further detail 2026-10-30-f0dbe129

06 **DLP Intent visibility into suspicious behavior** NEW — 30

Endpoint DLP 26.08 adds DLP Intent visibility into suspicious user behavior and into sensitive files entering endpoints.

— Thin description, no mechanism or UI path given 2026-10-30-f0dbe129

07 **Refreshed User Investigation experience** IMPROVED — 20

Endpoint DLP 26.08 adds a refreshed User Investigation experience.

— No specifics on what changed in the UI 2026-10-30-f0dbe129

└──▷ **BREAKING ON UPGRADE**

! Existing Zoom tenants onboarding AI transcript and AI meeting summary scanning must add additional scopes, webhook subscriptions, and reauthorize their Zoom integration.

WAS THIS USEFUL? 👍 👎

# Zscaler Private Access

Feedback ⓘ

changelog · Oct 30, 2026 BLOG ↗ RANK

Zscaler Private Access is a zero-trust network access service that securely connects users to internal applications without exposing the corporate network to the internet.

> Zscaler Private Access rolled out two FedRAMP-limited-availability additions to Application Segments: usage reporting and AI-powered segment recommendations.

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

01 **Application Segments usage reporting and AI recommendations**

NEW 69

Admins can view or download Application Segments Usage reports from the Zscaler Admin Console (navigate to Application Segments > Usage, then View or Download ) to see which segments are active and which user groups are accessing them; this requires the Segmentation add-on and is available for FedRAMP Moderate and High. Also added are AI-powered recommendations that analyze user logs and suggest application segments based on application similarity or user behavior, helping discover new segments and find missing applications for existing ones, also for FedRAMP Moderate and High.

Identify unused application segments and audit which user groups are accessing active ones — useful for access hygiene reviews.

📍 In the Zscaler Admin Console, go to Application Segments › Usage, then select View or Download to export the Application Segments Usage report.

— Names exact UI path and add-on requirement, but lacks AI mechanism details.

2026-10-30-959152fa

WAS THIS USEFUL? 👍 👎

◆ Backup & Recovery

# Veeam Kasten

Feedback ⓘ 9.0.10 NOTES ↗ RANK

Veeam Kasten is a Kubernetes-native platform for backing up, restoring, and migrating containerized applications and their persistent data.

> Kasten K10 9.0.10 adds a restore-side blueprint hook for pre-restore lifecycle control and a Presets filter on the Policies page, alongside several breaking changes around OpenShift support, STS endpoints, and immutability protection.

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

## 01 restorePrehook blueprint action NEW

93

Adds the `restorePrehook` blueprint action, the restore-side counterpart to `backupPrehook`, assignable via a `BlueprintBinding` or the `kanister.kasten.io/blueprint` annotation. It is called once before each matched resource is restored to quiesce operator-managed applications, remove finalizers, or delete conflicting resources, and aborts the restore if it fails.

Quiesce an operator-managed application before restore by wiring a `restorePrehook` action to matching resources via an annotation on the workload.

```
$ kubectl annotate deployment my-app
kanister.kasten.io/blueprint=my-blueprint
```

— Names exact action, binding mechanism, and failure behavior with runnable example.

9.0.10

## 02 Regional STS endpoint for VDC Vault AWS profiles BREAKING

70

VDC Vault AWS location profiles using the Registration authentication method now request credentials from the regional STS endpoint (e.g. `sts.eu-south-1.amazonaws.com`) instead of the global `sts.amazonaws.com`; environments that restrict outbound traffic must allow access to these regional endpoints.

— Names exact endpoint pattern and the network change required. 9.0.10

## 03 Immutability protection applied across shared location profiles

65

BREAKING

If two location profiles point at the same object store location and only one has an immutability protection period, Kasten K10 now applies that protection period to backups using the other profile too; if that profile's credentials lack immutable-backup permissions, its backups will fail until those permissions are added.

— Explains mechanism and failure condition but no config surface to act on directly.

9.0.10

04 **OpenShift 4.16/4.17 support removed** BREAKING 60

Support for Red Hat OpenShift 4.16 and 4.17 has been removed; users must upgrade to OpenShift 4.18 or later before upgrading Veeam Kasten.

— Clear version numbers and required migration action. 9.0.10

THINNER COVERAGE BELOW

05 **Presets filter on Policies page** NEW 50

Adds a Presets filter to the Policies page, letting users filter policies by one or more presets, by any preset, or by no preset.

— Describes the filter options but only a UI path, no further mechanism. 9.0.10

└──▷ **BREAKING ON UPGRADE**

! Support for Red Hat OpenShift 4.16 and 4.17 has been removed; upgrade to OpenShift 4.18 or later before upgrading Veeam Kasten.

! VDC Vault AWS location profiles using the Registration authentication method now request credentials from the regional STS endpoint (e.g. `sts.eu-south-1.amazonaws.com`) instead of `sts.amazonaws.com`; environments that restrict outbound traffic must allow access to these regional endpoints.

! If two location profiles point at the same object store location and only one has an immutability protection period, Kasten K10 now applies that protection period to backups using the other profile too; if that profile's credentials lack immutable-backup permissions, its backups will fail until those permissions are added.

WAS THIS USEFUL?  

## GOVERNANCE, RISK & COMPLIANCE

◆ Integrated & IT Risk Management

# CISO Assistant

Feedback ⓘ v4.2.0 NOTES ↗ RANK

CISO Assistant is a one-stop-shop GRC platform for Risk Management, AppSec, Compliance & Audit, TPRM, BIA, Privacy, and Reporting. It supports 200+ global frameworks with automatic control mapping, including ISO 27001, NIST CSF, SOC 2, CIS, PCI DSS, NIS2, DORA, GDPR, HIPAA, CMMC, and more.

> CISO Assistant's v4.2.0 release adds six new compliance frameworks, expands EBIOS RM exports with Workshop 5 data, enforces evidence attachments on questionnaire responses, and extends localization and TPRM capabilities.

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

01 **Folders API filter by ref_id** IMPROVED 70

Filter folders by `ref_id` via the folders API to narrow folder lookups programmatically.

— Names exact API parameter, immediately usable v4.2.0

02 **Six new compliance frameworks added to library** NEW 65

Add the `Czech Decree 409/2025` framework and `ZoKB` risk matrix, the `PIPEDA` framework ( `Schedule 1` , verbatim official text), the `MonServiceSécurisé` framework, the `NCA DCC-1:2022` (Data Cybersecurity Controls) framework, the `NCA CSCC-1:2019` (Critical Systems Cybersecurity Controls) framework, and OWASP Top 10 Web (2025) to the library.

— Names every framework added, but no detail on mapping mechanics v4.2.0

THINNER COVERAGE BELOW

03 **UI localization for Norwegian, Italian and Turkish** NEW 55

Add Norwegian Bokmål ( `nb` ) UI localization, including forms, tables, and dynamic strings; add `Italian` translations for vendor evaluation quick forms and `DPIA` workflows; and complete `Turkish` localization.

— Names languages and covered areas but no usage mechanism v4.2.0

04 **TPRM module gains custom fields and vendor visuals** NEW 55

Add custom fields and labels on entity assessments, plus vendor posture visuals with tier-based display, in the `TPRM` module.

— Names module and two additions, lacks configuration detail v4.2.0

05 **Per-audit PDF report template override** NEW — 55

Override the PDF audit report template (Typst-based) per audit in the Pro edition.

— Names mechanism (Typst) and edition scope, no exact steps v4.2.0

06 **Evidence required on questionnaire responses** NEW — 50

Require evidence attachments on questionnaire responses before submission.

— Clear behaviour change, no config key or toggle named v4.2.0

07 **EBIOS RM export includes Workshop 5** IMPROVED — 40

Expand EBIOS RM exports to now include Workshop 5 data.

— States what changed but not export format or access path v4.2.0

08 **Libraries moved under Catalog in sidebar** BREAKING — 40

The Libraries navigation entry is now located under Catalog in the sidebar.

— Exact navigation change, no further rationale given v4.2.0

09 **Portals editor supports documents** IMPROVED — 35

Improve the portals editor with support for documents.

— Vague on what document support entails v4.2.0

10 **Notifications cover additional event types** IMPROVED — 20

Expand notifications to cover additional event types.

— No specific event types or mechanism named v4.2.0

└──▷ **BREAKING ON UPGRADE**

! The Libraries navigation entry is now located under Catalog in the sidebar.

WAS THIS USEFUL?  

## DEPLOY

◆ Agentic Infrastructure

# microsandbox

Feedback ⓘ v0.7.12 NOTES ↗ RANK

easy, fast, programmable and local-first microVM runtime and library

> microsandbox v0.7.12 adds support for running nested virtualization inside sandboxes.

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

01 **Nested virtualization in sandboxes** NEW 30

Sandboxes can now run with nested virtualization enabled, allowing guest VMs to host their own hypervisor workloads.

— Describes capability but no config flag or setup steps given v0.7.12

WAS THIS USEFUL? 👍 👎

## OTHER / UNCATEGORIZED

◆ UNCATEGORIZED

## Arcade

Feedback ⓘ announced · Oct 29, 2026 BLOG ↗

Arcade is the actions runtime for enterprise AI agents â one control point to enforce, execute, and govern every action, every time.

Arcade adds MCP Apps, rendering interactive editors for Gmail, Slack, and Outlook Mail inside the chat, with file upload/download support and policy-enforced UI controls.

Arcade now supports MCP Apps, an extension to the Model Context Protocol that renders interactive interfaces (forms, editors, dashboards) inside the chat client instead of requiring tab-switching.

NEW INTEGRATION File uploads and downloads now work inside MCP Apps by running the app code locally, opening the native file picker and writing large files straight to disk — already available in the Slack, Gmail, and Outlook Mail apps.

Authorization and governance rules are enforced at the point when the MCP App interface is built and again at the point of action, so UI controls (such as a Send button) are only shown when the user's permissions allow the underlying tool call.

WAS THIS USEFUL? 👍 👎

// END OF TRANSMISSION

The Cyber Toolchain · curated daily · November 1, 2026
Releases & features from the open-source and commercial cyber tools that practitioners actually run.

▷ Subscribe Feedback on this issue