



H1 2026 Cloud and SaaS Reliability Report

30,246 outages. 1,082 providers. January - June 2026.

IncidentHub

Methodology

- Data comes from public status pages only, via APIs, webhooks, RSS, and other methods. Private status monitoring for Microsoft Azure and Microsoft 365 is also done, but those numbers are not used here.
- An outage starts when a provider posts degraded performance, a minor issue or a major issue, and closes when the provider marks it resolved.
- Outage duration runs from the provider's first acknowledgment to their resolution timestamp. All times are in UTC.
- The dataset has fixed boundaries: 1,082 providers with continuous coverage from January 1 to June 30 2026. Providers added mid-period are out of scope.
- Maintenance windows are excluded.

This report does not rank providers. Each provider decides what goes on its status page and at what granularity. E.g., Cloudflare has hundreds of edge locations, and a localized outage in one POP still counts as one outage. These counts measure status page activity, not customer impact.

H1 2026 at a Glance

30 , 246

outages tracked

1 , 082

providers

15 . 9%

had zero outages in H1

6 , 070

in May, the worst month

4 , 723

cloud provider outages, across 86 providers

9 . 44

average outages per provider in May, across the 643 with at least one

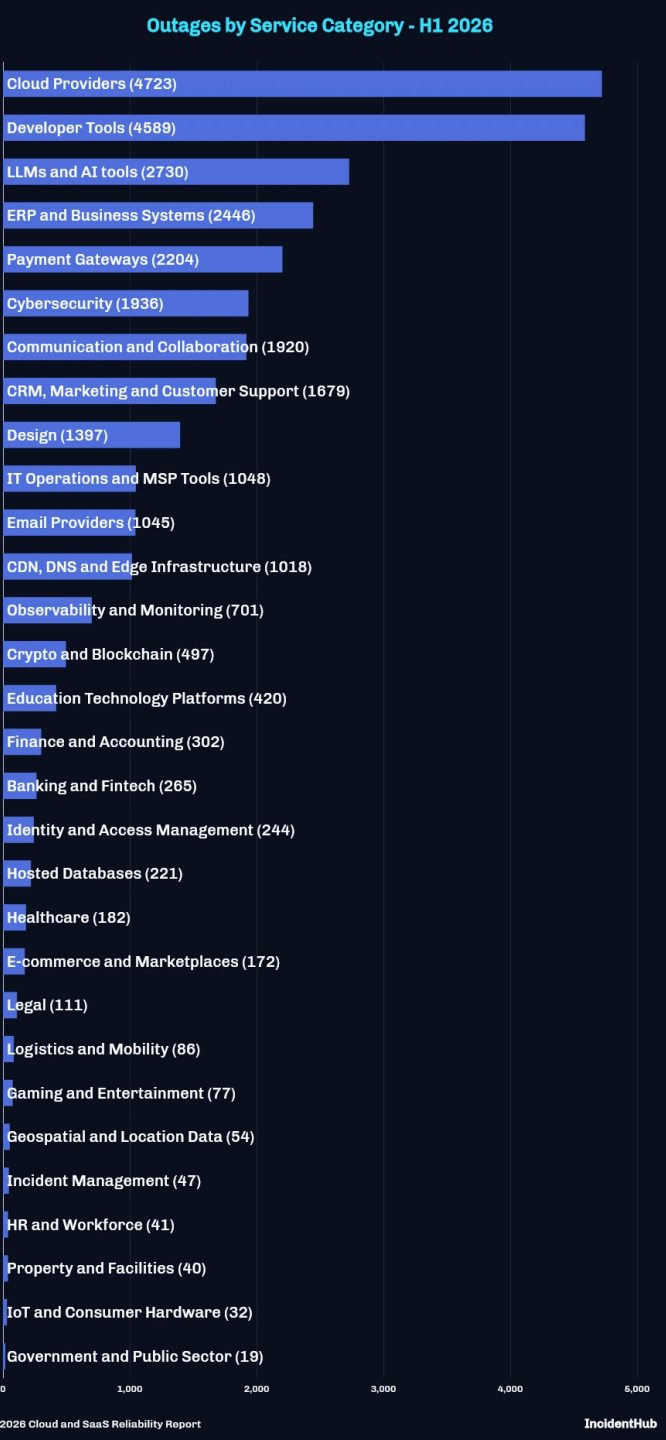
Cloud Providers and Developer Tools were also the two categories most often citing an upstream provider outage as the root cause.

Cloud and Developer Tools Lead, with a Small Gap

- **Cloud Providers: 4,723** across 86 providers
- **Developer Tools: 4,589** across 187 providers

Developer tools reach that number across more than twice as many providers, so the per-provider picture differs from the totals.

Providers that span categories are counted once in the most relevant category. So AWS sits under Cloud Providers, not CDN or DNS.

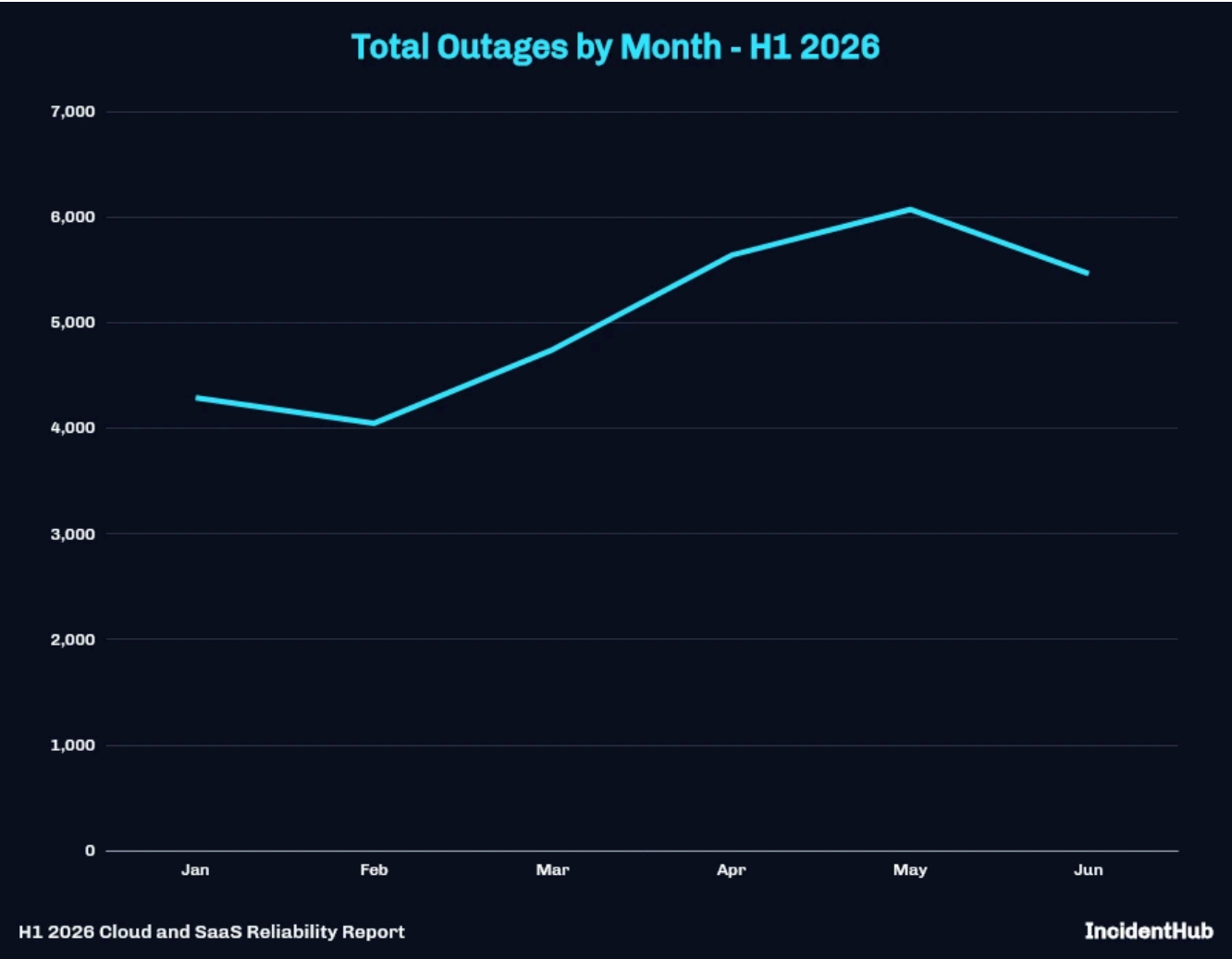


Total Outages Peaked in May, at 6,070

Cloud provider outages peaked in May too, at 1,139 across 67 providers. Their upward trend from January to May slowed down in June.

Shorter outages under an hour are becoming more common, whereas the band up to 24 hours has stayed roughly flat.

Chart shows total outages per month across all tracked providers.



Cloud Providers

4,723

86

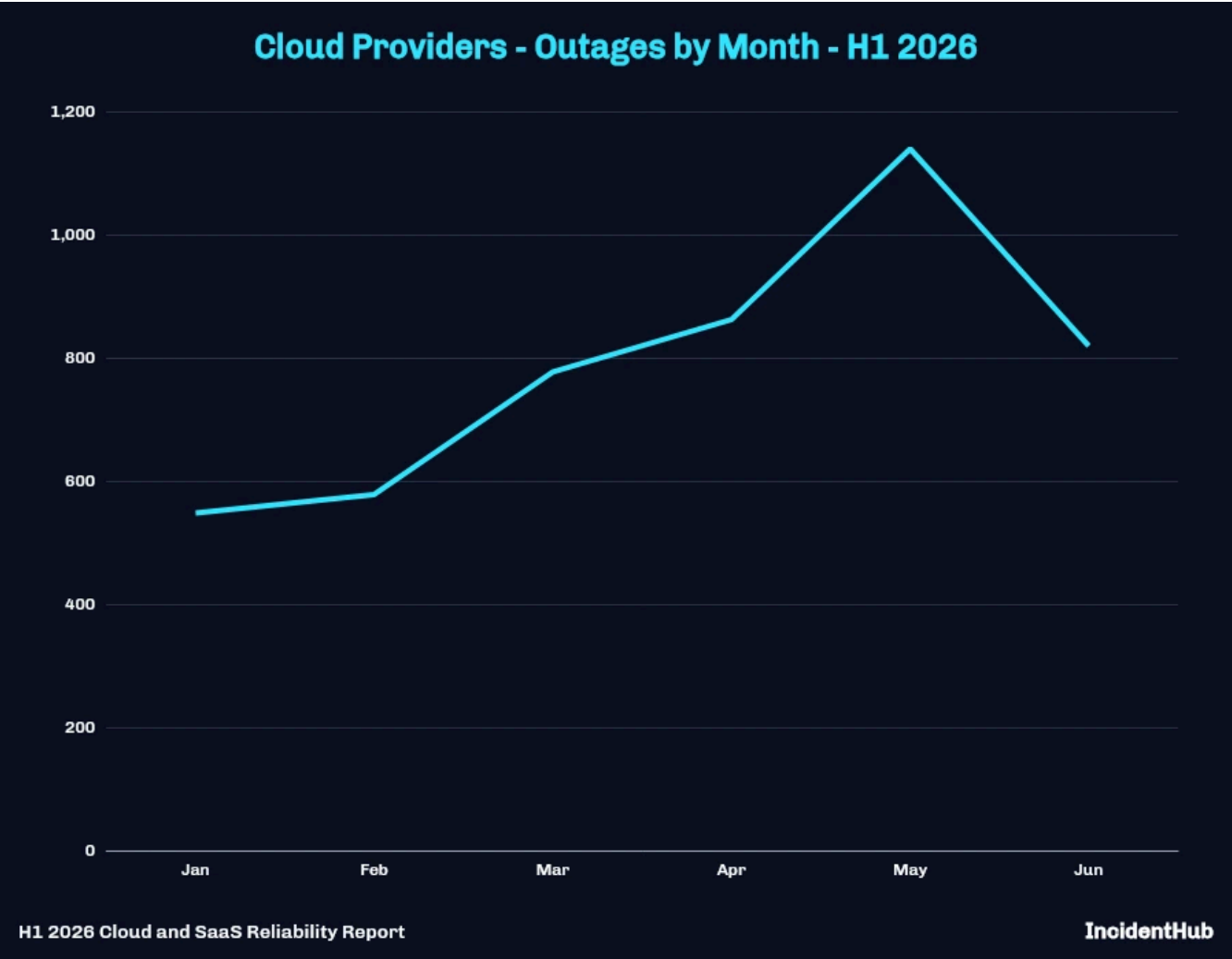
outages

providers

Tracked incidents for H1 2026:

Provider	Incidents
AWS	14
GCP	2
Azure	14
OCI	2

Azure's figure is public status page data only. These four are not comparable with each other: a lower count may mean a provider publishes only widespread incidents, or groups into one entry what another posts as several.



Two Failures That Volume Does Not Capture

AWS Middle East, March

AWS reported physical damage to me-central-1 and me-south-1 from drone strikes in the armed conflict.

Salesforce migrated user data to its Sweden region over 3+ weeks. Confluent advised customers to move out workloads to other regions.

AWS now describes me-central-1 as unable to reliably support customer applications and me-south-1 as unavailable, with billing suspended in both and restoration expected to take several months.

Railway and GCP, May 19

At 22:20 UTC, Google Cloud automatically suspended Railway's production account, taking down their API, control plane and databases. Edge proxies kept serving from cached routing tables until those expired, at which point every workload became unreachable, including healthy ones on Railway Metal and AWS.

Around 8 hours to recovery. The failure mode is an upstream provider acting automatically without notice.

Edge, CDN and DNS: Upstream Multipliers

1,018

16

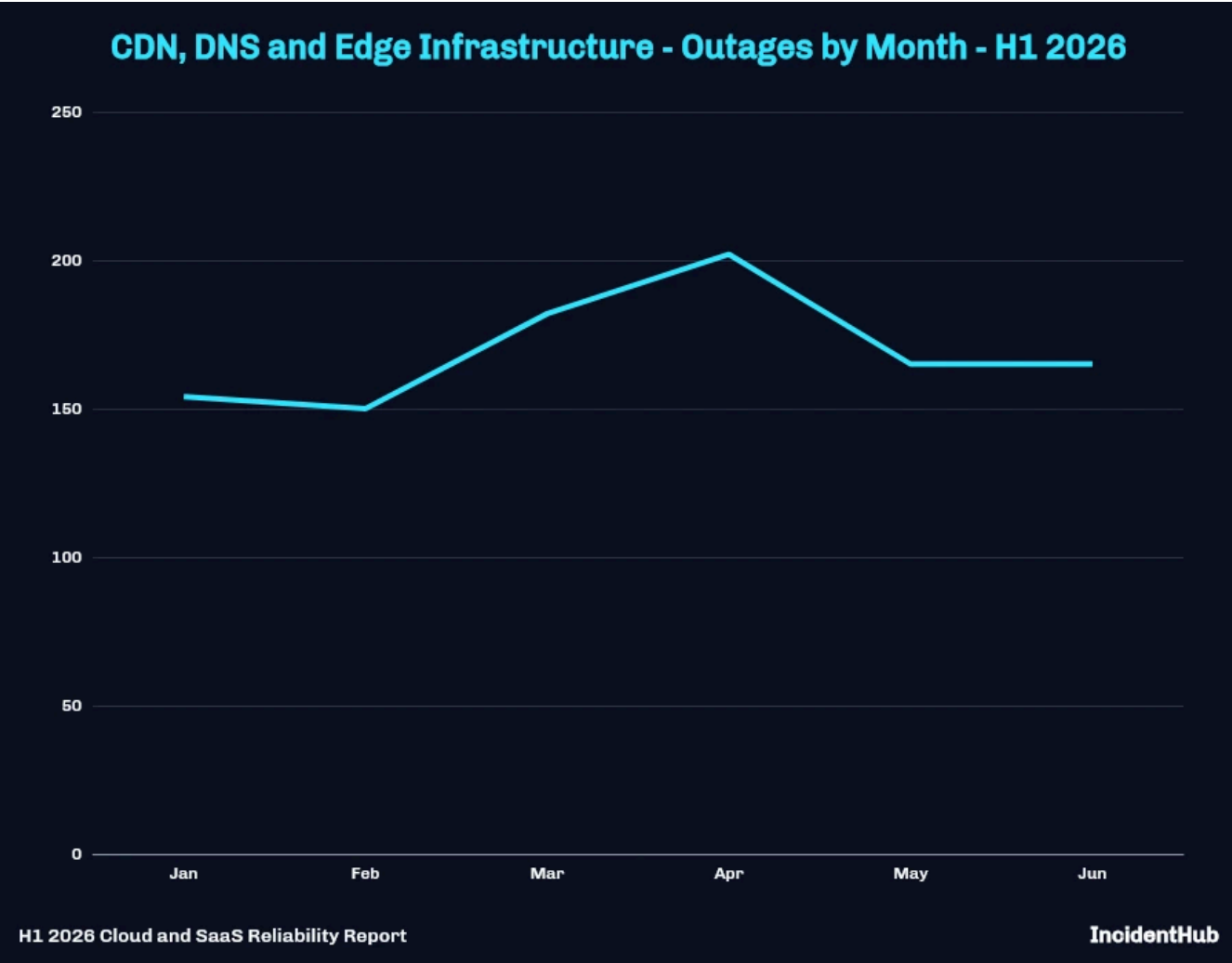
outages

providers

- Cloudflare: 487, peaking at 98 in April
- Fastly: 161, peaking in January and April
- Akamai: 59, peaking in April
- DNS-related: 73 across 30 providers

A well-engineered application can still be unavailable if its CDN returns errors or its DNS stops resolving.

Counts are not comparable across these three. Edge network sizes differ, and so does POP-level status page granularity. DNS-related outages span categories, including cloud providers with DNS services.



IAM: The Login Chokepoint

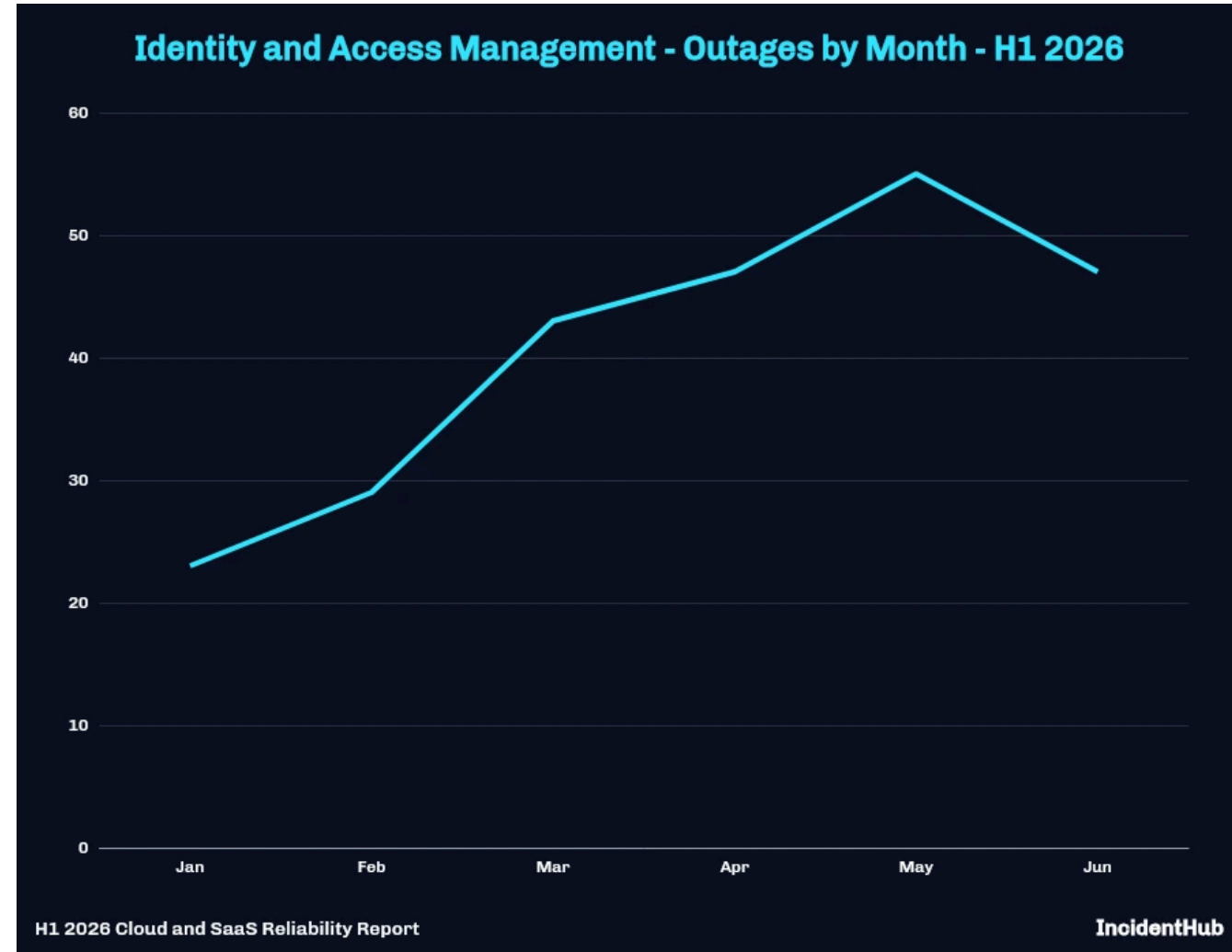
244 **16**
outages providers

Rising through H1 and peaking in May. Okta recorded 13, Auth0 19.

Confirmed downstream impact, from the providers' own incident reports:

- Cloudflare dashboard logins, via Okta
- Draftbit, via Clerk
- Harness Traceable logins, via Auth0
- Nintex Workflow logins, via an identity provider

The service can be running and still be unusable if nobody can log in.



AI Providers Are Now in the Critical Path

2,730

34

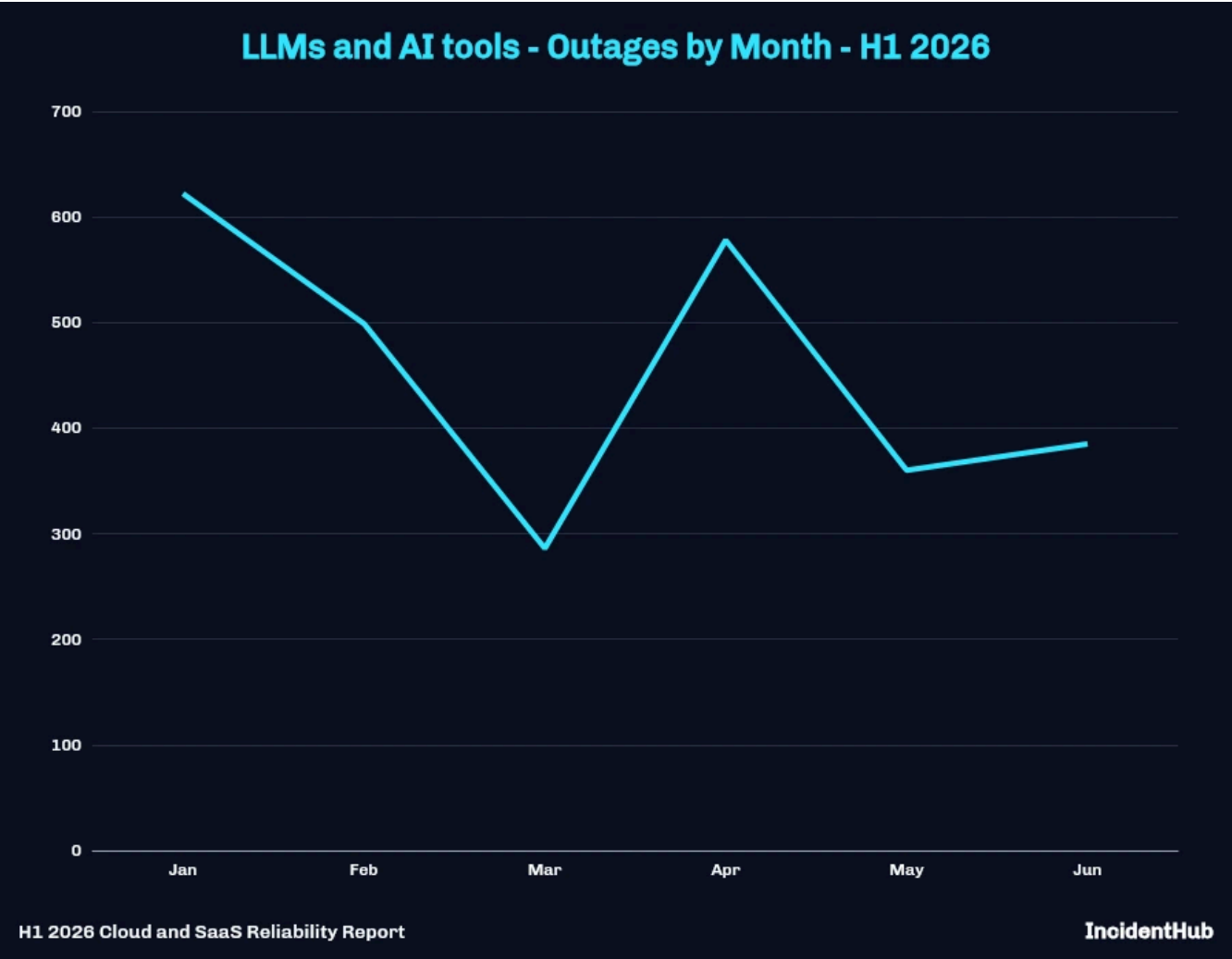
outages

providers

Developer tooling often runs multiple AI providers for fallback. Customer support, communication and productivity products usually do not, which leaves them with little to fall back on.

The Fable 5 and Mythos 5 Suspension

Anthropic suspended access from June 13 at 00:50 UTC to July 1 at 19:26 UTC, 18 days 19 hours, in compliance with an export control directive. Not an outage in the true sense, but four downstream providers posted incident reports: AWS Bedrock, Notion, GitLab.com and Netlify's AI Gateway.



Four More Categories

Developer Tools

4,589 **187**
outages providers

Peaked in March at 844, from 135 providers. GitHub 169, GitLab 72, Bitbucket 10, with GitHub Actions the worst affected component at 37.

Payment Infrastructure

2,204 **33**
outages providers

Trending up since January, peaking in June. Stripe peaked at 11 in March and again in May. FedACH's March 3 outage delayed file distribution and settlement for multiple ACH windows, affecting Stripe and others.

Communication and Collaboration

1,920 **75**
outages providers

Zoom 131, Slack 57. Visible across the whole organization, and on the same channels used to coordinate incident response.

Observability and Monitoring

701 **34**
outages providers

Incident management tools saw a further 47 outages across 4 providers. An outage in either group means a slowdown or a complete loss of visibility into whether something else is wrong.

EdTech Platforms

420

38

outages

providers

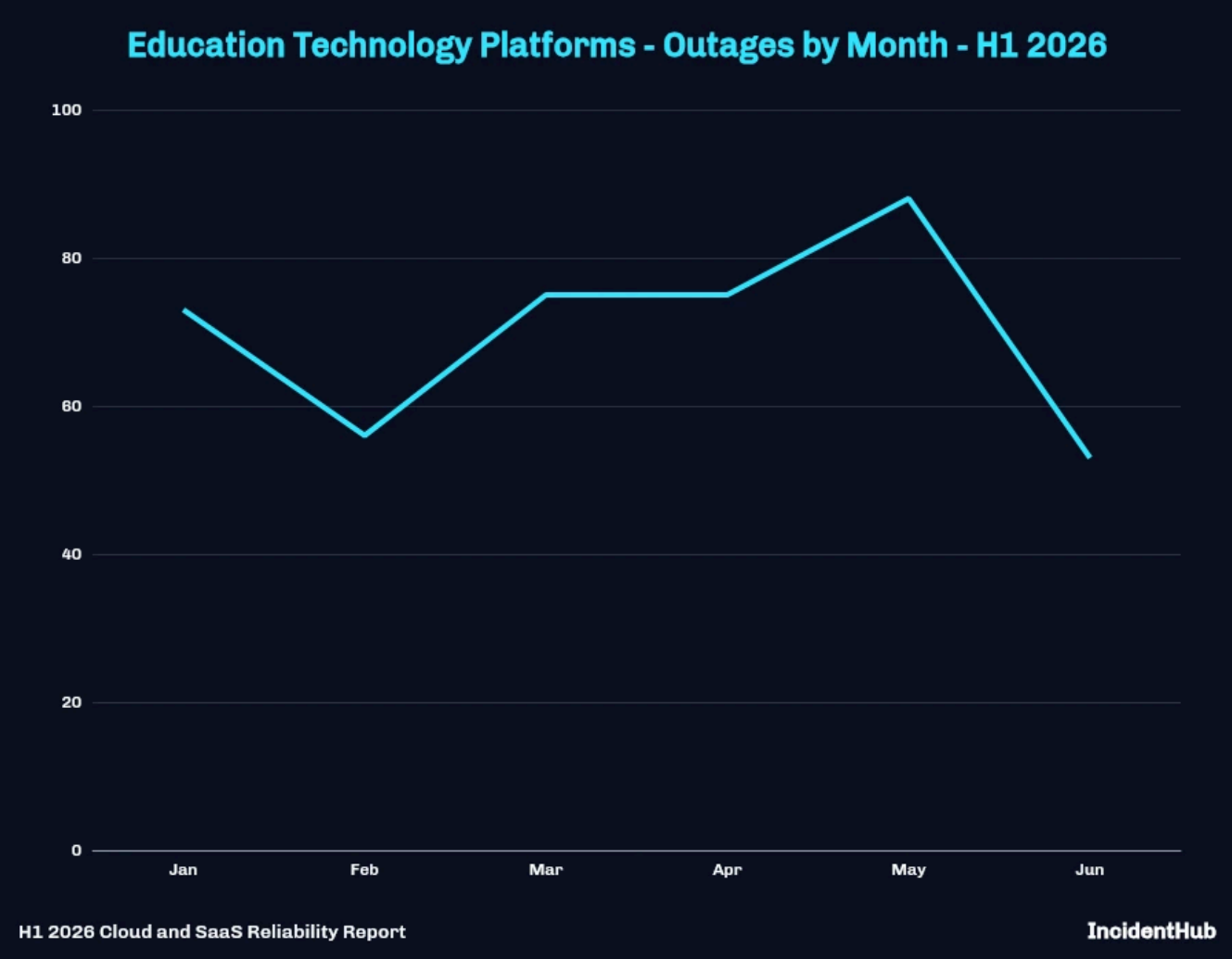
Academic calendars are fixed so an outage during an exam window cannot be rescheduled around. EdTech also inherits the AI dependency, on top of infrastructure and auth.

Canvas, May 2026

A security incident attributed to a ransomware group took Instructure's Canvas platform down for institutions worldwide, including during final exam periods at some colleges and universities. The group claimed around 9,000 institutions were affected. Instructure later said it had blocked the unauthorized access and closed the vulnerabilities and relevant privilege escalation paths.

H1 2026 showed that security-triggered outages, not just infrastructure failures, can take platforms offline at scale.

Education Technology Platforms - Outages by Month - H1 2026



Four Patterns Across the Data

- 1. Localized triggers propagate globally.** Control planes built for fast replication move a misconfiguration at the speed of a good one. Azure's February 2026 remediation policy, GCP's June 2025 quota update, and Cloudflare's November 2025 Bot Management file all followed this pattern.
- 2. Automated policy enforcement is its own risk category.** Railway and GCP in May 2026, and UniSuper's GCVE infrastructure in 2024 under different circumstances.
- 3. Control plane resilience matters more than data plane resilience.** Healthy VMs and databases are unusable if the control plane that manages them is down. Multi-cloud is often touted as the answer, but it carries its own complexity and your dependencies may not be multi-cloud either.
- 4. Recovery generates its own load.** Queued jobs, thundering herds and third-party rate limiting on a recovering service can extend an outage well past the original fault.

H1 2026 Was Defined by Dependency Risk

Across 30,246 outages and 1,082 providers, many outages with wide reach started one layer upstream, in an edge network, an identity provider, an LLM API or a cloud control plane.

The practical takeaway is to know your first- and second-order dependencies, and watch them in one place.

incidenthub.cloud

IncidentHub is not affiliated with any of the services and vendors mentioned. All logos and company names are trademarks of their respective holders. Charts are generated from IncidentHub's aggregated data; reuse with attribution. Full report: <https://blog.incidenthub.cloud/h1-2026-cloud-saas-reliability-report>