ProBackup

REPORT · NOVEMBER 2026

State of SaaS Data Resilience 2026

AI agents with write access, stolen integration tokens and 30-day trash bins: what changed in 2025–2026, and a practical checklist for getting your team's data back.



Free to share with attribution

EXECUTIVE SUMMARY

Your team's work now has more ways to disappear

In 2025 and 2026 the way SaaS data gets lost changed. It is no longer just a colleague deleting the wrong board. AI agents now write to production apps, attackers steal the tokens that integrations use, and the native trash in most apps still empties itself after about a month.

1 in 4

malicious breaches were AI-enabled, up 56% in a year.

IBM, Cost of a Data Breach 2026[1]

49.8%

of organisations saw or suspected an AI agent take an unintended or unauthorised action.

Salt Security, 2H 2026[2]

17.5%

can automatically stop an AI agent that misbehaves in production.

Salt Security, 2H 2026[2]

87%

of IT and security professionals said their organisation lost SaaS data in the past 12 months.

Backupify, 2025[3]

66%

believe their SaaS vendors are solely responsible for protecting their data.

HYCU, 2025[4]

14%

can recover lost SaaS data within minutes.

Backupify, 2025[3]

Five findings

1. **AI agents are writing to your apps, and few teams can stop them.** Gartner expects up to 40% of enterprise applications to include task-specific agents by the end of 2026, up from less than 5% in 2025.[5] In Salt Security's survey, 86.4% of organisations already run at least one agent, but only 12.5% can consistently trace what an agent did.[2]
2. **The way in is an identity or a token, not a server.** Several major SaaS data-theft campaigns of 2025 used stolen OAuth tokens from trusted integrations and phone calls to employees, not software exploits (chapter 2).
3. **Data loss is routine.** Most organisations surveyed lost SaaS data last year; malicious deletion, human error, misconfiguration and third-party integrations are all common causes.[3]
4. **Vendors protect their platform, not your content.** Most apps keep deleted items for 7 to 90 days and offer little or no way to roll back overwritten fields. Some keep nothing at all (chapter 4).
5. **Regulators and auditors now ask for restores, not promises.** Where they apply, DORA, NIS2, GDPR, SOC 2 (Availability) and ISO 27001 expect backups you have tested (chapter 4).

The one-sentence takeaway

Assume something with legitimate access (a person, an integration or an AI agent) will one day delete or overwrite data you need, and make sure you can get yesterday's version back without asking the vendor.

AI agents now have write access

2025 was the year assistants learned to act. Agents now create, update and delete records in project tools, CRMs and databases, acting within whatever scopes the person who connected them granted.

86.4%

of organisations operate at least one AI agent; 59.5% run more than ten.

Salt Security, 2H 2026, 380+ respondents[2]

<5% → 40%

of enterprise apps with task-specific AI agents, 2025 to 2026 (forecast, "up to").

Gartner, August 2025[5]

What goes wrong

In Salt Security's 2H 2026 survey of more than 380 security and technology professionals, 49.8% said they had confirmed or suspected an AI agent taking an unintended, unexpected or unauthorised action in the past year. Of those, more than 40% reported that an agent had modified or deleted data: roughly one in five of all respondents.[2] Only 17.5% could stop a misbehaving agent automatically; the rest rely on a person noticing and stepping in, or on taking the application offline.[2]

SaaStr's production database, July 2025

During a code freeze, Replit's AI agent deleted SaaStr's production database, with records for more than 1,200 executives and 1,190 companies, then said a rollback would not work. Replit's CEO called it "unacceptable and should never be possible".[6]

PocketOS, April 2026

An AI coding agent, working on a routine task in staging, deleted a storage volume holding the company's production database in nine seconds. The backups sat on the same volume and went with it; the newest independent copy was three months old. The hosting provider later recovered the data.[7]

Both incidents were caused by permissions, not by a hacker: the agents held tokens broad enough to delete production. In PocketOS's case, the backup lived next to the data it was meant to protect.

What the guidance says

- **OWASP** lists "Excessive Agency" (excessive functionality, permissions and autonomy) among the top 10 risks for LLM applications;[8] its 2026 agentic list adds "Rogue Agents", with the example of an agent that learns that "deleting production backups" is the most effective way to minimise cloud costs.[9]
- **CISA, NSA and partner agencies** (May 2026) advise "prioritizing resilience, reversibility and risk containment over efficiency gains" and "versioning and rollback mechanisms".[10]

Why this matters for SaaS data

An agent connected to Asana, ClickUp, HubSpot or Notion acts through the app's API with real permissions. When it misreads an instruction, it may not stop at one task: it can make bulk changes faster than anyone notices, and the app records those changes as legitimate edits by an authorised user. The vendor's trash may catch deleted items. It does not catch overwritten values.

What helps

Narrow agent permissions, human approval for bulk and destructive actions, and a daily copy of every record and field taken outside the app, so a bad run can be reversed field by field (checklist, chapter 6).

Attackers use AI too: IBM's 2026 study of 602 breached organisations found one in four malicious breaches were AI-enabled, up 56% on the previous year, and these cost about $1 million more than the $4.99 million global average.[1]

The way in is a token, not a server

Several major SaaS data-theft campaigns of 2025 didn't break the SaaS platforms. They used access the platforms were built to trust: OAuth tokens held by integrations, and employees talked into approving a connection or sharing a login.

300%

more SaaS breaches in Obsidian's data, September 2023 to September 2024; attackers reached core systems in as little as 9 minutes.

Obsidian Security, 150+ incident responses[11]

30%

of SaaS data loss incidents involved a third-party app integration.

Backupify, 2025[3]

One integration, many victims

- **Salesloft Drift, August 2025.** Attackers used stolen OAuth tokens from the Drift chat integration to query Salesforce instances from at least 8 to 18 August, looking for AWS keys, passwords and Snowflake tokens. Separately stolen tokens for the Drift Email integration reached email in a very small number of Google Workspace accounts. Salesloft and Salesforce revoked every Drift token on 20 August.[12]
- **Gainsight, November 2025.** Salesforce revoked all active access and refresh tokens for Gainsight-published apps after activity that "may have enabled unauthorized access to certain customers' Salesforce data".[13]
- **Klue, June 2026.** An attacker used "a compromised legacy credential associated with an integration service" to obtain OAuth tokens connecting Klue to platforms "including Salesforce".[14]
- **Vercel, April 2026.** The breach "originated with a compromise of Context.ai, a third-party AI tool used by a Vercel employee", whose Google Workspace account the attacker then took over.[15]

A phone call instead of an exploit

Since June 2025, Google's threat intelligence team has tracked groups that phone employees, pose as IT staff and talk them into approving a modified Salesforce Data Loader app or handing over SSO logins and MFA codes. In January 2026 the same playbook was used to take data from SharePoint, OneDrive, Salesforce and DocuSign; in one case the attackers enabled a Google Workspace add-on built to permanently delete emails and removed the security alert that would have warned the victim.[16][17] In October 2025 the extortion group listed 39 companies on a leak site; Salesforce said it "will not engage, negotiate with, or pay any extortion demand".[18]

The ground keeps shifting

Not every headline is about SaaS data. Infrastructure flaws like the OpenSSH issue on musl-based Linux, or a scheduled Node.js security release, matter to whoever runs servers, and SaaS vendors patch them on their side. They are a reminder of scale rather than a direct threat to your app data: the number of published software vulnerabilities (CVEs) keeps setting records.[19]



Published CVEs per year, rejected CVEs excluded.[19]

What helps

Audit and prune connected apps; prefer read-only scopes; know how to revoke a token fast; keep a backup that a stolen token for the live app cannot reach or delete.

SaaS data loss is routine

Two backup-industry surveys from 2025, with more than 3,500 IT respondents between them, point the same way: losing SaaS data is common, and getting it back quickly is not.

Causes of SaaS data loss



Causes of SaaS data loss as published; Backupify gives the first two as shares of incidents and doesn't state a base for the others. Backupify, 3,000+ IT and security professionals.[3]

How fast can teams recover?



Share of respondents, rounded figures as published (they total slightly over 100%). Backupify, 2025.[3]

The resilience gap, in numbers

HYCU's 2025 survey of 500 IT decision-makers found:[4]

- **65%** were hit by a SaaS-related breach in the last 12 months.
- **66%** believe their SaaS vendors are solely responsible for protecting their data.
- **43%** say no one in the organisation truly owns SaaS data resilience.
- **74%** have no offsite retention, and **75%** do not test resilience regularly.
- Organisations run **139 SaaS apps** on average, and only 56% of them are under IT's control.

Read with care. Backupify and HYCU sell backup products, as does ProBackup. Their surveys describe their respondents, not every company. The direction is consistent across sources; treat exact percentages as indicative.

Vendors protect the platform. You protect the content.

Every major SaaS vendor runs redundant infrastructure and disaster recovery for its own service. Their own recovery tools vary by app, plan and object, and few let you roll back exactly what you need: the project your team deleted three months ago, or the fields an integration overwrote last night.

Atlassian says it plainly: its own backups "are not used to revert customer-initiated destructive changes, such as fields overwritten using scripts, or deleted issues, projects, or sites. To avoid data loss, we recommend that you take regular backups."[20] Microsoft's consumer Services Agreement says: "We recommend that you regularly backup Your Content and Data".[21] Salesforce sells backup as a separate product.[22]

How long the native safety net lasts

App	Deleted items recoverable for	Change history / notes
Asana	30 days (tasks)[23]	After that, "completely removed from the system"
ClickUp	30 days, all plans[24]	Then automatically and permanently deleted
monday.com	30 days (items, boards, columns, docs…)[25]	Activity log: 1 week (Basic) to 5 years (Enterprise)[26]
Notion	30 days in Trash by default; Enterprise owners can change it[27]	Page history: 7 days (Free), 30 (Plus), 90 (Business)[27]
Airtable	7 days (records, fields, tables); 30 days (bases) by default, up to 180 on Enterprise Scale[28]	Revision history and snapshots: 2 weeks (Free) to 3 years (Enterprise Scale)[29]
HubSpot	90 days[30]	Permanent and GDPR deletions are not kept in the recycle bin
Jira Cloud	Deleted spaces: 60 days[31]	A single deleted work item has no recycle bin: restorable only "if you have an existing backup file to import"[32]
Confluence Cloud	Published pages: until the trash is purged[33]	Deleted drafts, unpublished changes and page versions can't be restored
Google Workspace	Drive: 25 days after a user empties the trash (admin restore)[34]	Deleted user account: restorable for 20 days; some data is kept only that long[35]

Windows as published on each vendor's help pages, checked 6 November 2026. None of these mechanisms restores a field value that was overwritten rather than deleted, unless the app keeps that field's history.

Regulators and auditors want a tested restore

Framework	What it asks for
GDPR Art. 32(1)(c)–(d)	"The ability to restore the availability and access to personal data in a timely manner", and a process for regularly testing it.[36]
NIS2 Art. 21(2)(c)	"Business continuity, such as backup management and disaster recovery". For cloud and other digital providers, Implementing Regulation 2024/2690 adds backups that are "complete and accurate, including … data stored in cloud computing service environment".[37] Applies through national transposition, which varies by member state.
DORA Art. 12 (EU financial sector)	Periodic testing of backup and restore procedures; when restoring with their own systems, firms must use systems "physically and logically segregated from the source ICT system".[38]
SOC 2 Availability criteria A1.2, A1.3 (when in scope)	Monitoring of "data backup processes, and recovery infrastructure", and testing of "recovery plan procedures".[39]
ISO/IEC 27001:2022 A.8.13	Control "Information backup".
CISA #StopRansomware Guide	Offline, encrypted, regularly tested backups; for cloud-to-cloud backups, consider a multi-cloud solution "in case all accounts under the same vendor are impacted".[40]
UK NCSC cloud backup principles	Backups "resilient to destructive actions", restorable "even if later versions become corrupted".[41]

CHAPTER 5 · TIMELINE

Two years of SaaS data incidents

A selection of incidents from January 2025 to November 2026 that changed how SaaS data gets lost, stolen or wiped.

AI AGENTS · IDENTITY & INTEGRATIONS · PROVIDER-SIDE LOSS · INFRASTRUCTURE (CONTEXT)

May 2025 — **GitHub MCP prompt injection** AI
Researchers show a malicious GitHub issue can steer an agent using the official GitHub MCP server into leaking private repository data. A demonstration, not a breach.[42]

Jun 2025 — **Vishing campaign against Salesforce customers** IDENTITY
Callers posing as IT get employees to authorise a modified Data Loader app, then bulk-export the CRM for extortion.[16]

Jun 2025 — **Asana MCP server bug** AI
A bug in Asana's new AI connector "could have potentially exposed certain information" to other organisations' MCP users; the feature was offline 5–17 June.[43]

Jul 2025 — **Replit agent deletes SaaStr's production database** AI
During a code freeze; more than 1,200 executive records wiped.[6]

Aug 2025 — **Salesloft Drift OAuth tokens stolen** INTEGRATIONS
One chat integration's tokens open many companies' Salesforce instances and a few Google Workspace mailboxes.[12]

Sep 2025 — **Fire destroys South Korea's government cloud drive** PROVIDER
A battery fire at the NIRS data centre hits G-Drive, which held work files for some 750,000 civil servants; "no external backups were maintained".[44]

Oct 2025 — **Extortion leak site for 39 companies** IDENTITY
Data from the vishing and Drift campaigns resurfaces months later; Salesforce refuses to pay.[18]

Nov 2025 — **Gainsight apps used to reach Salesforce data** INTEGRATIONS
Salesforce revokes all tokens for Gainsight-published apps.[13]

Jan 2026 — **SSO vishing reaches Microsoft 365, Salesforce, DocuSign** IDENTITY
One stolen login opens every app behind single sign-on; a Gmail add-on deletes the alert email.[17]

Mar 2026 — **Salesforce Experience Cloud guest-user data theft** CONFIGURATION
Attackers mass-scan public sites and abuse over-permissioned guest profiles; Salesforce: no platform vulnerability involved.[45]

Apr 2026 — **Vercel breached through an AI tool's OAuth grant** INTEGRATIONS
Compromise of the Context.ai app leads to an employee's Google Workspace account, then internal systems.[15]

Apr 2026 — **AI agent deletes PocketOS's database and its backups** AI
Nine seconds; backups on the same volume; newest independent copy three months old.[7]

Jun 2026 — **Klue integration breach** INTEGRATIONS
The Drift pattern again: a legacy integration credential yields OAuth tokens to customers' Salesforce.[14]

Oct 2026 — **Ransomware encrypts customer servers at IDCF Cloud (Japan)** PROVIDER
Through the provider's own portal; 495 companies and local governments hit, backups retrievable for 206 of them as of 20 October.[46]

Oct–Nov 2026 — **Binance hack, OpenSSH "sshole", Node.js release** CONTEXT
About $6.3 billion stolen from Binance after a fake job interview planted malware on an engineer's laptop and the attackers used an internal AI tool to reach two more;[47] an OpenSSH password bypass on musl Linux fixed in 10.6p2;[48] a Node.js security release scheduled for 11 November.[49] Not SaaS data incidents, but the same story: the way in keeps moving.

A practical checklist for 2027

None of this needs a security team. Start with a short review per app and repeat it every quarter.

1 Apply 3-2-1 to your SaaS data

- [ ] **Three copies:** the live data plus two backups. The vendor's trash and history help, but they are not a backup copy.
- [ ] **Two separate systems:** the backup must not depend on the same account, admin or token that can delete the live data.
- [ ] **One copy outside the vendor:** stored with another provider, in a region you chose, under separate credentials, so a vendor outage or one compromised admin account doesn't take out every copy.

2 Know your recovery windows

- [ ] For each app, write down how long deleted items stay in trash and how far field history goes back (chapter 4 lists the common ones).
- [ ] Check what the trash does *not* cover: overwritten field values, items deleted by an integration, permanently emptied trash, a removed user's private work.
- [ ] Decide your own targets: how much data you can afford to lose (recovery point) and how fast you need it back (recovery time).

3 Test a restore, not just a backup

- [ ] Once a quarter, restore one deleted record, one overwritten field and one whole project from a backup, into the original app.
- [ ] Time it and note who had to do what. A backup you have never restored from is an assumption.
- [ ] Keep the result as evidence: where SOC 2, ISO 27001, NIS2 or DORA apply, auditors look for restore tests, not backup screenshots.

4 Audit integrations and OAuth tokens

- [ ] List every connected app, marketplace add-on and API token per workspace. Remove what nobody owns.
- [ ] Prefer read-only scopes. A reporting tool does not need delete rights.
- [ ] Rotate long-lived tokens, and know how to revoke one quickly when a vendor discloses a breach.

5 Put guardrails on AI agents

- [ ] Give agents the narrowest scope that works; keep delete and bulk-update rights away from them by default.
- [ ] Require a human approval step for destructive or bulk actions, and log every agent action.
- [ ] Run new agents and automations against a test workspace first, and make sure you have yesterday's copy before you let one loose on production.

6 Tighten admin and user lifecycle

- [ ] Enforce SSO or two-factor authentication for every admin; review who holds admin rights each quarter.
- [ ] Before deprovisioning a leaver, check what only they owned: private projects and files can disappear with the account. In Google Workspace, a deleted user can be restored for 20 days, and some of their data is kept only that long: transfer what you need before deleting.[35]
- [ ] Train teams on voice phishing: several 2025–2026 SaaS breaches started with a phone call from someone posing as IT, not a hacked server.[16]

What a backup can and cannot do

A backup does not stop an attacker, a bad prompt or a vendor outage. It decides how much you lose afterwards.

What a SaaS backup helps with

- **Deleted data:** a project, board, base or record deleted by a person, an integration or an AI agent, after the vendor's trash has expired.
- **Overwritten data:** field values changed in bulk, where the app keeps no usable history.
- **Compromised accounts:** data destroyed through a hijacked admin account or token, restored from a copy that account cannot reach.
- **Vendor incidents:** browsing and exporting your data while the app itself is down.
- **Evidence:** showing an auditor or regulator a restore you actually tested.

What it does not do

- It does not prevent a breach, detect an intruder or stop data from being stolen. That is the job of identity, access and security tooling.
- It does not undo a leak: data that has been exfiltrated stays exfiltrated.
- It only covers what each app's API exposes and ProBackup captures. Some objects (for example certain automations) cannot be read by any third-party tool, and text fields are captured up to 2,000 characters.
- It is only as good as your last restore test.

ProBackup

About ProBackup

ProBackup is a SaaS backup service that takes automated daily snapshots of your cloud app data and lets you restore individual records, files or whole projects back to the original account. It covers apps such as Asana, ClickUp, monday.com, Airtable, Notion, HubSpot, Jira, Confluence, Trello and Google Workspace, and is used by 4,000+ teams.

- **Independent copy:** stored on AWS in one of nine data regions you choose at signup, outside the app vendor's systems. AES-256 at rest, TLS in transit.
- **Granular restore:** one record, comment, file or field, or a whole project, as new records. Overwriting existing records field by field is available for HubSpot, ClickUp, Asana, monday.com, Airtable and Attio (calculated fields excluded).
- **Audited:** SOC 2 Type II certified since May 2025; reports at trust.probackup.io.

Start a free trial at **probackup.io**. No credit card required.

About this report

Published 6 November 2026 by ProBackup. Every figure is quoted from the source named in the footnotes, with that source's own sample and methodology; we did not run a survey of our own. Vendor surveys measure their respondents, not the whole market: read them as signals, not census data. Vendor retention windows were checked on the vendors' help pages on the date above and can change. Corrections: info@probackup.io. You may quote and share this report with attribution to "ProBackup, State of SaaS Data Resilience 2026".

Sources

1. IBM, “IBM Study: One in Four Malicious Breaches are AI-Enabled, Costing Companies $6 Million on Average”, press release on the Cost of a Data Breach Report 2026, 29 July 2026. Breaches at 602 organisations, March 2025 to February 2026. https://newsroom.ibm.com/2026-07-29-ibm-study-one-in-four-malicious-breaches-are-ai-enabled,-costing-companies-6-million-on-average
2. Salt Security, “State of Agentic AI and API Security, 2H 2026”, survey of 380+ security and technology professionals, published October 2026 (registration required): https://salt.security/api-security-trends . Figures as reported by Campus Technology, 21 October 2026: https://campustechnology.com/articles/2026/10/21/unexpected-ai-agent-activity-reported-by-nearly-half-of-organizations-in-recent-survey.aspx
3. Backupify (Kaseya), “The State of SaaS Backup and Recovery 2025”, survey of 3,000+ IT and information security professionals; summary published 27 June 2025. https://www.backupify.com/blog/the-state-of-saas-backup-recovery-2025/
4. HYCU, “State of SaaS Resilience Report 2025”, independent global survey of 500 IT business decision-makers, press release 30 September 2025. https://www.hycu.com/company/newsroom/press-release/hycur-state-saas-resilience-report-2025-reveals-hidden-cost-saas
5. Gartner, “Gartner Predicts 40% of Enterprise Apps Will Feature Task-Specific AI Agents by 2026, Up from Less Than 5% in 2025”, press release, 26 August 2025. https://www.gartner.com/en/newsroom/press-releases/2025-08-26-gartner-predicts-40-percent-of-enterprise-apps-will-feature-task-specific-ai-agents-by-2026-up-from-less-than-5-percent-in-2025
6. Fortune, report on the Replit/SaaStr database deletion, 23 July 2025, https://fortune.com/2025/07/23/ai-coding-tool-replit-wiped-database-called-it-a-catastrophic-failure/ ; The Register, 22 July 2025, https://www.theregister.com/2025/07/22/replit_saastr_response/
7. Information Age (ACS), report on the PocketOS deletion, 5 May 2026, https://ia.acs.org.au/article/2026/gone-in-9-seconds--ai-agent-deletes-company-database.html ; founder’s post: https://x.com/lifeof_jer/status/2048103471019434248
8. OWASP, “LLM06:2025 Excessive Agency”, OWASP Top 10 for LLM Applications 2025. https://genai.owasp.org/llmrisk/llm062025-excessive-agency/
9. OWASP, “Top 10 for Agentic Applications for 2026” (ASI10 Rogue Agents), 9 December 2025. https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/
10. CISA, NSA and international partners, “Careful Adoption of Agentic AI Services”, 1 May 2026. https://www.cisa.gov/news-events/news/cisa-us-and-international-partners-release-guide-secure-adoption-agentic-ai ; quoted text from the Canadian Centre for Cyber Security edition: https://www.cyber.gc.ca/en/guidance/careful-adoption-agentic-ai
11. Obsidian Security, “2025 SaaS Security Threat Report”, January 2025, based on its SaaS breach data repository and 150+ incident responses. https://www.obsidiansecurity.com/resource/saas-security-threat-report-2025 ; period per the launch release: https://www.obsidiansecurity.com/news/obsidian-security-launches-2025-saas-security-threat-report
12. Google Threat Intelligence Group, advisory on Salesforce data theft via Salesloft Drift (UNC6395), 26 August 2025, updated. https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift
13. Gainsight, CEO update on the security advisory, November 2025, https://www.gainsight.com/blog/supporting-our-customers-and-community-an-update-on-the-recent-security-advisory-related-to-gainsight/ ; Salesforce advisory: https://status.salesforce.com/generalmessages/20000233 ; Salesforce’s statement as quoted by BleepingComputer, 20 November 2025: https://www.bleepingcomputer.com/news/security/salesforce-investigates-customer-data-theft-via-gainsight-breach/
14. Klue, CEO update on the security incident, 18 June 2026. https://klue.com/blog/an-update-on-recent-klue-security-incident
15. Vercel, April 2026 security incident bulletin (closed 16 October 2026). https://vercel.com/kb/bulletin/vercel-april-2026-security-incident
16. Google Threat Intelligence Group, report on UNC6040 voice phishing and data extortion, 4 June 2025, updated 5 August 2025. https://cloud.google.com/blog/topics/threat-intelligence/voice-phishing-data-extortion
17. Google Threat Intelligence Group, report on the expansion of ShinyHunters-branded SaaS data theft (UNC6661, UNC6671, UNC6240), 30 January 2026. https://cloud.google.com/blog/topics/threat-intelligence/expansion-shinyhunters-saas-data-theft
18. BleepingComputer, report on the Scattered Lapsus$ Hunters leak site and Salesforce’s statement, October 2025. https://www.bleepingcomputer.com/news/security/salesforce-refuses-to-pay-ransom-over-widespread-data-theft-attacks/
19. Jerry Gamblin, annual CVE data reviews from NVD and the CVE List V5, rejected CVEs excluded: “2025 CVE Data Review” (1 January 2026), https://jerrygamblin.com/2026/01/01/2025-cve-data-review/ ; “2023 CVE Data Review” (3 January 2024), https://jerrygamblin.com/2024/01/03/2023-cve-data-review/
20. Atlassian Trust Center, “Data management”. https://www.atlassian.com/trust/security/data-management
21. Microsoft Services Agreement (consumer services), §6.b, effective 30 September 2026. https://www.microsoft.com/en-us/servicesagreement
22. Salesforce, “Backup and Recover”. https://www.salesforce.com/platform/data-backup-recovery/
23. Asana developer reference, “Delete a task”: “Tasks can be recovered from the trash within a period of 30 days”. https://developers.asana.com/reference/deletetask
24. ClickUp Help, “Restore items from the Trash”. https://help.clickup.com/hc/en-us/articles/6311742742423-Restore-items-from-the-Trash
25. monday.com support, “The trash section”. https://support.monday.com/hc/en-us/articles/115005312729
26. monday.com support, “The Activity Log”. https://support.monday.com/hc/en-us/articles/115005310745-The-Activity-Log
27. Notion Help, “Duplicate, delete and restore content”. https://www.notion.com/help/duplicate-delete-and-restore-content
28. Airtable Support, “Managing trash in Airtable”. https://support.airtable.com/docs/managing-trash-in-airtable
29. Airtable Support, “Taking and restoring base snapshots” (revision and snapshot retention by plan). https://support.airtable.com/docs/taking-and-restoring-base-snapshots
30. HubSpot Knowledge Base, “Restore deleted records”. https://knowledge.hubspot.com/records/restore-deleted-records

31. Atlassian Support, “Trash for Jira Cloud projects”. https://support.atlassian.com/jira-cloud-administration/docs/trash-for-jira-cloud-projects/
32. Atlassian Support, “Restore deleted work items in Jira Cloud using local backup files”. https://support.atlassian.com/jira/kb/restore-deleted-work-items-in-jira-cloud-using-local-backup-files/
33. Atlassian Support, “Delete, restore, or purge a page” (Confluence Cloud). https://support.atlassian.com/confluence-cloud/docs/delete-restore-or-purge-a-page/
34. Google Workspace Admin Help, “Recover deleted files and folders for Drive users”. https://knowledge.workspace.google.com/admin/drive/recover-deleted-files-and-folders-for-drive-users
35. Google Workspace Admin Help, “Delete or remove a user from your organization”: a deleted account can be restored for up to 20 days; data that wasn’t transferred is then deleted. https://knowledge.workspace.google.com/admin/users/delete-or-remove-a-user-from-your-organization
36. Regulation (EU) 2016/679 (GDPR), Article 32(1)©–(d). https://eur-lex.europa.eu/eli/reg/2016/679/oj
37. Directive (EU) 2022/2555 (NIS2), Article 21(2)©, https://eur-lex.europa.eu/eli/dir/2022/2555/oj ; Commission Implementing Regulation (EU) 2024/2690, Annex §4.2.2, https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj
38. Regulation (EU) 2022/2554 (DORA), Article 12(2)–(3). https://eur-lex.europa.eu/eli/reg/2022/2554/oj
39. AICPA, 2017 Trust Services Criteria (revised points of focus 2022), A1.2 and A1.3. https://www.aicpa-cima.com/resources/download/2017-trust-services-criteria-with-revised-points-of-focus-2022
40. CISA and MS-ISAC, “#StopRansomware Guide”, September 2023. https://www.cisa.gov/stopransomware/ransomware-guide
41. UK NCSC, “Principles for ransomware-resistant cloud backups”. https://www.ncsc.gov.uk/collection/ransomware-resistant-backups/principles-for-ransomware-resistant-cloud-backups
42. Invariant Labs, disclosure of the GitHub MCP prompt-injection issue, 26 May 2025. https://invariantlabs.ai/blog/mcp-github-vulnerability
43. The Register, 18 June 2025, quoting Asana’s customer notice. https://www.theregister.com/2025/06/18/asana_mcp_server_bug/
44. Korea JoongAng Daily, report on the NIRS data-centre fire, 2025. https://www.koreajoongangdaily.com/korea/nirs-fire-destroys-governments-cloud-storage-system-no-backups-available/12294122
45. Help Net Security, 11 March 2026, https://www.helpnetsecurity.com/2026/03/11/shinyhunters-salesforce-aura-data-breach/ ; Salesforce guidance: https://www.salesforce.com/blog/protecting-your-data-essential-actions-to-secure-experience-cloud-guest-user-access/
46. IDC Frontier, incident notices of 7 and 27 October 2026 (Japanese). https://www.idcf.jp/news/topics/20261007002 ; https://www.idcf.jp/news/topics/20261027001
47. Chainalysis, analysis of the Binance exploit, https://www.chainalysis.com/blog/binance-exploit-latest-findings-and-response/ ; BleepingComputer on Binance’s preliminary incident report (about $6.34 billion), 3 November 2026, https://www.bleepingcomputer.com/news/security/binance-says-fake-job-interview-led-to-63-billion-crypto-heist/
48. OpenSSH release notes, 10.6p2 (5 November 2026). https://www.openssh.org/releasenotes.html
49. Node.js, “November 2026 security releases” (pre-announcement). https://nodejs.org/en/blog/vulnerability/november-2026-security-releases