WHITE PAPER FOR DECISION-MAKERS

What big software vendors *won't tell you.*

"If we go with the big, well-known vendors, we're safe." This paper shows why that assumption can be expensive — with 12 documented, publicly reported cases from 2021–2025, and the independent architecture that would have contained the damage.

12	2021–25	$5.4B	12/12
DOCUMENTED CASES	ALL RECENT, ALL PUBLIC	SINGLE WORST CASE*	ARCHITECTURE-AVOIDABLE

> *The structural difference isn't "big vendor" vs. "small vendor." It's whether you own the platform your business runs on — or rent it on someone else's terms.*

* CrowdStrike, July 2024: ~$5.4B in direct losses to the Fortune 500 from a single faulty vendor update (Parametrix). Every figure in this paper comes from public reporting; sources are listed on the final page. This document is informational and not legal or financial advice.

THE 3-MINUTE VERSION

01 Executive summary

Every business now runs on software it does not own. That is normal — and, handled carelessly, it is the single largest operational risk most companies never put on a risk register. This paper documents twelve recent, public cases in which dependence on a software vendor turned into a direct business problem: sudden price increases with no negotiating room, data made inaccessible by someone else's mistake, a breach at one vendor cascading into thousands of customers, and platforms simply switched off.

The pattern is consistent. The harm is rarely the technology failing — it is the **loss of control**: you can't see the problem, can't set the priority, can't take your data and leave. In each of the twelve cases, an architecture built on ownership, open formats, and independent backups would have contained the damage. Not prevented every incident — contained it.

> **WHAT THIS PAPER IS — AND ISN'T**
>
> It is not an argument that the cloud is bad or that big vendors are incompetent. It is an argument that **concentration of control is a risk you can price** — and reduce. The fix isn't fear; it's architecture.

The three questions this paper answers

- How does dependence actually build — and where does it bite? **(Section 2)**
- What has it cost real companies, with sources? **(Section 3 — the 12 cases)**
- What architecture contains the damage — and why the popular "fixes" don't? **(Sections 4–5)**

HOW DEPENDENCE BUILDS

02 The three mechanisms of dependence

Dependence rarely arrives as a decision. It accumulates — one tool, one subscription, one integration at a time — until three mechanisms quietly take hold.

01 Pricing power

Once your operations run on a platform, the vendor sets the price and you have no real alternative on short notice. Renewals arrive as take-it-or-leave-it. Microsoft 365 raised commercial prices for the first time in a decade in 2022 (Business Standard $12.50→$15), then layered a $30/user Copilot add-on on top. Broadcom collapsed VMware's catalog into four subscription bundles; some customers reported renewal increases of 500–1,000%+.

02 Exit cost & lock-in

Leaving is harder than joining — by design. Data lives in proprietary formats; permissions, integrations, and history were never cleanly exportable. The harder the exit, the more a price increase becomes something you simply absorb. That friction *is* the product.

03 Single point of control

When a vendor controls the platform, one decision or one mistake on their side — an outage, a deletion, a breach, an account suspension, a discontinued product — instantly becomes your problem, with no way to intervene, reprioritize, or recover on your own timeline.

THE THROUGHLINE

None of these is about a vendor being "bad." Each is a structural consequence of not owning the platform. Section 3 shows what happens when the structure is tested.

03 Twelve cases, with sources

Each is recent, public, and verifiable. Figures are as reported by the sources on the final page.

01 CROWDSTRIKE · JUL 2024

One update, a global outage

A single faulty security-software update crashed millions of Windows machines worldwide, grounding flights and halting hospitals and banks.

~$5.4B direct losses to the Fortune 500 (excl. Microsoft); ~10–20% insured.

Parametrix · Cybersecurity Dive · Fortune

02 GOOGLE CLOUD / UNISUPER · MAY 2024

A $135B fund deleted — backups too

A misconfiguration during provisioning deleted UniSuper's entire cloud subscription, including in-cloud backups. ~2 weeks offline.

647,000 members locked out; recovered only thanks to an **independent third-party backup**.

The Register · Data Center Dynamics

03 MOVEIT / CL0P · 2023

One tool, thousands of victims

A flaw in a single managed file-transfer product let one ransomware crew breach organizations downstream en masse.

2,500+ organizations, ~93M individuals; Emsisoft est. $10B+ total cost.

Emsisoft · TechCrunch · CSO Online

04 BROADCOM / VMWARE · 2023–24

Perpetual licenses, gone overnight

After the $61B acquisition, perpetual licenses were discontinued and products forced into subscription bundles.

AT&T alleged a **1,050%** increase; Siemens, Tesco & others also sued.

CIO Dive · TechTarget

05 LASTPASS · 2022

The vaults were stolen after all

Attackers exfiltrated backups of customer password vaults via a compromised engineer's device — first downplayed, later confirmed.

~30M vaults exposed; feds linked a **$150M** crypto heist; $24.5M class settlement.

Krebs on Security · Sophos

06 ATLASSIAN · APR 2022

An internal script deleted live sites

A maintenance script run with the wrong IDs deleted ~400 customers' cloud sites. Rebuilt by hand over up to two weeks.

Backups existed but **didn't cover configs/integrations** — manual rebuilds.

The Register · Pragmatic Engineer

03 Twelve cases, with sources (cont.)

07 OKTA · OCT 2023

A breach at your identity provider

Attackers reached Okta's support case-management system; session tokens in support files enabled hijacking attempts downstream.

Contact data of **all ~18,400** support customers exposed; 1Password, BeyondTrust, Cloudflare hit.

Krebs on Security · The Record

08 MICROSOFT 365 · 2022 & 2024

The rent goes up — on schedule

First commercial price rise since 2011 (+~20%), then a mandatory-feeling $30/user Copilot add-on, then further increases announced.

Recurring, vendor-set increases with **no negotiating leverage** at renewal.

CNBC · Petri · Directions on Microsoft

09 ADOBE · 2024

Easy to start, hard to cancel

The U.S. DOJ/FTC sued Adobe over allegedly hidden early-termination fees and a deliberately difficult cancellation flow.

Lock-in **by contract design**, not just by data — now a federal lawsuit.

FTC.gov · Reuters

10 AWS / PARLER · JAN 2021

Switched off with ~24 hours' notice

Regardless of the politics, the mechanism is the lesson: a hosting provider terminated service and the application went dark overnight.

Your uptime can depend on a **vendor's terms-of-service decision**.

The Verge · AWS court filings

11 GOOGLE "GRAVEYARD" · ONGOING

The product you built on, discontinued

Stadia shut down (2023); Google Domains was sold to Squarespace (2023); IoT Core was retired (2022). The catalog of killed products keeps growing.

Strategic dependence on a product the vendor can **simply end**.

killedbygoogle.com · Ars Technica

12 ORACLE & SAP AUDITS · ONGOING

The licensing audit as a revenue tool

"Indirect access" and metric reinterpretations turn routine audits into large true-up bills — e.g. SAP's UK case over Diageo's indirect use.

Costs you **didn't agree to up front**, enforced by audit leverage.

The Register · Computer Weekly

THE COMMON THREAD

Different vendors, different failure modes — one root cause: the customer didn't control the platform, the data, or the exit. The next section addresses the fixes most companies reach for first.

WHY THE POPULAR FIXES FALL SHORT

04 The false fixes

When the risk becomes visible, companies usually reach for two answers. Both reduce one worry while leaving the core dependence intact.

"WE'LL GO MULTI-CLOUD"

Spreading workloads across two or three hyperscalers adds cost and complexity — and still leaves you renting on their formats, their pricing, and their terms. You now depend on more vendors, not fewer. It hedges an outage; it does not return control.

"WE'LL FIX IT WITH CONTRACT TERMS"

Addenda and SLAs help at the margins, but they don't give you the source code, the data in open formats, or the ability to run the system yourself. When the renewal or the audit comes, leverage still sits with the vendor.

THE TEST

For any proposed fix, ask one question: **if this vendor doubled the price, deleted our data, or shut the product down tomorrow, could we keep operating on our own terms?** If the answer is no, the dependence is unchanged — you've only rearranged it.

Real independence is not "a different vendor" or "more vendors." It is a change in **who holds control**: the server, the data, and the software. That is an architecture decision — the subject of the final section.

05 What would have contained the damage

The same four principles recur across all twelve cases. None requires heroics — only that ownership and control sit with you.

01

Own the platform

The server runs in your name, on your contract. A vendor can't suspend, delete, or re-price what you own. (Cases 02, 04, 08, 10.)

02

Open formats & standard software

Open-source standards any administrator can run mean no proprietary lock-in and a real, low-friction exit. (Cases 04, 08, 09.)

03

Independent, tested backups

Backups at a second, separate provider — and actually restored on a schedule — survive a provider's mistake. Exactly what saved UniSuper. (Cases 02, 06.)

04

Isolation & least privilege

Single-tenant operation and per-application isolation stop one breach from becoming all of them. (Cases 03, 05, 07.)

THE POINT

An independent architecture would not have prevented every incident in this paper. But in each of the twelve, it would have **contained the damage** — turning a business-threatening event into a managed one with a plan, a backup, and a way out.

NEXT STEP

See where you stand — before you decide anything.

The NexaStack Independence Audit maps your dependencies, vendor by vendor — flat $490, credited toward your first project. nexastack.co/en/audit

TRANSPARENCY

— Sources & methodology

Every case above is drawn from public reporting. Figures are as stated by these sources at time of publication; where estimates vary, we cite the conservative figure. This document is informational and not legal or financial advice.

01 · CrowdStrike — Parametrix; Cybersecurity Dive; Fortune; Axios (Jul–Aug 2024)

02 · UniSuper / Google Cloud — The Register; Data Center Dynamics; Keepit (May 2024)

03 · MOVEit / Cl0p — Emsisoft; TechCrunch; CSO Online (2023)

04 · Broadcom / VMware — CIO Dive; TechTarget; Network World (2023–24)

05 · LastPass — Krebs on Security; Sophos; Wikipedia (2022–25)

06 · Atlassian — The Register; The Pragmatic Engineer; BleepingComputer (Apr 2022)

07 · Okta — Krebs on Security; The Record; CSO Online (Oct–Nov 2023)

08 · Microsoft 365 — CNBC; Petri; Directions on Microsoft (2022–26)

09 · Adobe — U.S. FTC / DOJ; Reuters (Jun 2024)

10 · AWS / Parler — The Verge; AWS court filings (Jan 2021)

11 · Google discontinuations — killedbygoogle.com; Ars Technica (2022–23)

12 · Oracle & SAP audits — The Register; Computer Weekly (ongoing)

A NOTE ON FIGURES

We deliberately do not sum these into a single “total damages” number: the figures measure different things (direct losses, breach-cost estimates, settlement amounts, price increases) and aren’t additive. The point isn’t one headline number — it’s that the same structural risk recurs, at scale, across every category of vendor.

NexaStack

Own it, don’t rent it.

nexastack.co/en · hello@nexastack.co