# The **SaaS** Trap

## What Every CIO Needs to Know

Onymos

In 1999, Salesforce introduced the world to Software-as-a-Service (SaaS). "Introducing salesforce.com, the new Internet site that allows you to easily access, manage, and/or share all your organization's sales information - immediately, efficiently and reliably - right from your computer," read its homepage.

Since then, SaaS has transformed everything. Technology leaders have described it as the democratization of software. By 2030, the SaaS market is expected to be worth over $800 billion (USD)[1], up from $150 billion in 2020.

But there's a problem. SaaS is broken.

## The Biggest Cybersecurity Risk is SaaS Itself

At the beginning of 2023, NationsBenefits, US Wellness, Community Health Systems, and 127 other organizations experienced massive concurrent data breaches. Millions of their members, patients, and customers were affected.

Hackers didn't have to attack them all. In fact, their target was just one company — Fortra, a SaaS cybersecurity firm (ironically).

These organizations had all been using compromised Fortra-hosted file-transfer software. Unbeknownst to them, for three days between January 28th and January 30th, their files were being intercepted by Clop, an Eastern European hacker gang.

At least two of the companies affected by the hack told TechCrunch that Fortra initially downplayed the extent of the breach[2], allegedly going so far as to claim their data was completely safe. They only realized that wasn't true when Clop itself reached out to them demanding a ransom.

NationsBenefits was by far the hardest-hit company. Over 3 million of its members were impacted. Since then, multiple class-action lawsuits have been filed against Fortra and its hacked customers (by their customers.Fortra continues to publish cybersecurity tips on its website.

Incidents of vendor compromise like this are happening more frequently. Our 2024 SaaS Disruption Report found that 45% of respondents experienced a cybersecurity incident through a third-party SaaS solution in the past year. That fulfills a Gartner prediction that by 2025, "45% of organizations globally will have been victims of software supply chain attacks, marking a threefold increase from 2021."[3]

This is all because the SaaS ecosystems most of us rely on are only getting more complex and interconnected. That doesn't just make our third-party software vendors' security vulnerabilities our problem, it makes all of their mistakes our problem.

When CrowdStrike released a seemingly ordinary update in July 2024, its undetected "problematic content" inadvertently grounded over 5,000 flights, causing one of the most significant disruptions to air travel since 9/11.

The airlines who were affected had, essentially, outsourced control over their own products and services — and paid the price.

> “Even though it says 'Ford' on the front, I actually have to go to Bosch to get permission to change their seat control software”

Jim Farley
**CEO, Ford**

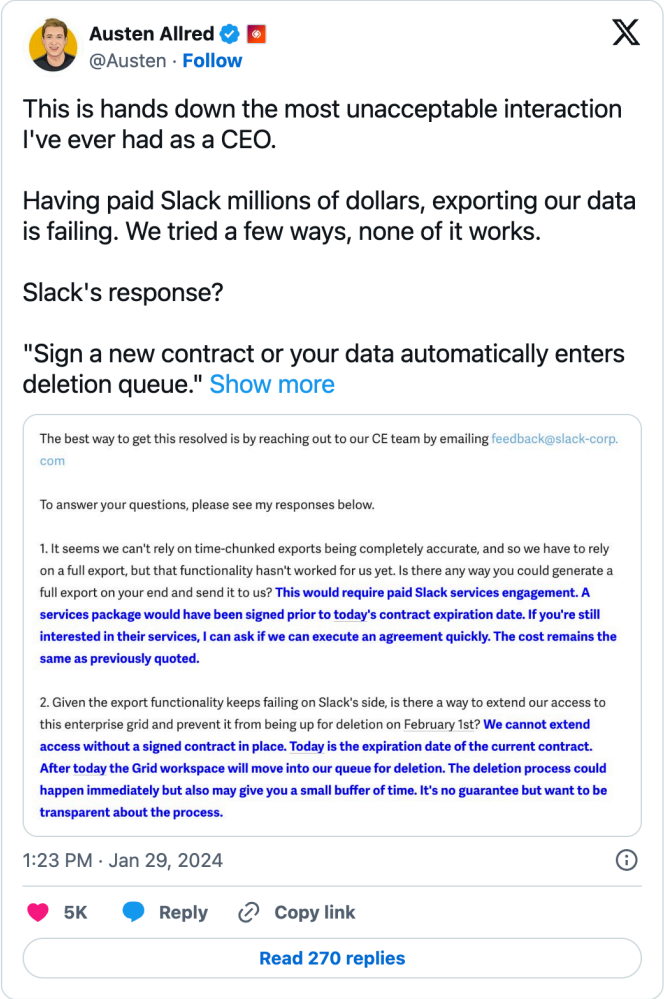
## SaaS Is Out of (Your) Control

If they had talked to Jim Farley, CEO of Ford, he might’ve warned them about outsourcing to third-parties. Ford isn't what most people think of when they think of a software company, but Farley is trying to change that, and he's candid about how relying on third-party software became a problem. When he appeared on the popular Fully Charged podcast last year, he explained, "We’ve farmed out the software modules that control the vehicles to our suppliers because we could bid them against each other... the problem is the software is all written by 150 different companies, and they don’t talk to each other... we can’t even understand it all. Even though it says 'Ford' on the front, I actually have to go to Bosch to get permission to change their seat control software.”

This lack of real ownership over our own products and services extends to the data they produce, too.

When Austen Allred, the CEO of polarizing code boot camp BloomTech, tried to migrate his virtual school off of Slack, he almost learned a $78,000 lesson on the concept of real ownership.

On X, he complained that Slack's data migration tools didn't work, but that Slack's Customer Experience team refused to help. They threatened to move years' worth of his online school's records into a deletion queue in just two days if he didn't pay for a $78,000 "services package."




Luckily for Allred, he was a prominent enough figure to prompt Slack's parent company's CEO, Salesforce's Marc Benioff, to personally DM him, apologize, and solve the problem.

Slack's website claims, "Customer Data (i.e. the messages, content and files that you submit to the Services) is owned and controlled by the Customer."

Allred might disagree.

## The SaaS Trap

There's a reason SaaS is so popular — it's so easy. Describing its benefits, IBM says you can "start using SaaS applications immediately, sometimes in minutes, for a minimal upfront cost."

It's no wonder then that most technology leaders think of SaaS as a key enabler of digital transformation. Deloitte estimates that "the right combination of digital transformation actions" could add up to $1.25 trillion in value across all Fortune 500 companies.[5] But there's the catch: "the right combination."

In 2022, McKinsey reported, "Nine in ten C-level and senior leaders say their organizations have pursued at least one large-scale digital transformation in the past two years."[4]

But, surprisingly, a majority of respondents revealed that those transformation projects had not had "the impact on revenue or

> "Nine in ten C-level and senior leaders say their organizations have pursued at least one large-scale digital transformation in the past two years."[4]
>
> **McKinsey Global Survey**



Onymos

## Hire tech-savvy leaders

## Implement bold strategies

## Don't rely on off-the-shelf tools (SaaS)

costs that they expected." The respondents employed by "top economic performers," however, were much more likely to report success.

So, what is "the right combination of digital transformation actions" that "top economic performers" are taking when they digitally transform? McKinsey tells us they're hiring tech-savvy leaders, implementing bold strategies — and not relying on off-the-shelf tools (SaaS).

In other words, SaaS is a trap for digital transformers. Those relying on SaaS are sacrificing security, ownership, and control. And it's not paying off.

> SaaS model as it is in 2024 needs to be completely transformed."

Shiva Nathan
**CEO, Onymos**

## SaaS Needs to Transform

Onymos Founder and CEO Shiva Nathan says the “SaaS model as it is in 2024 needs to be completely transformed. The way SaaS is supposed to work is that you pay money to receive service. Somewhere, something went wrong. Worldwide, folks pay money and data to receive service. We need to remove the ‘and data’ part from SaaS, keep the speed, and add trust.”

Onymos achieves that through its unique and award-winning “no-data” architecture (Onymos sees no data, and saves no data) and source code licensing model. It’s the opposite of vendor lock-in.

That’s why the world's biggest technology transformers trust Onymos — because we’re transforming SaaS.

**Contact Us To Learn More**

Shiva Nathan
**CEO, Onymos**

A seasoned technology executive and entrepreneur, Shiva Nathan draws from his experience as a software innovator to empower organizations to reach their digital transformation goals. Before founding Onymos, he was head of Intuit's Platforms and Services organization. He also held technical leadership positions at Oracle and CA Technologies, which continue to leverage the software products he helped define and build. Shiva earned his bachelor's degree with honors in computer engineering from BITS Pilani and an MBA from UC Berkeley's Haas School of Business.

**Sources**


[1] https://www.grandviewresearch.com/industry-analysis/saas-market-report

[2]https://techcrunch.com/2023/03/24/fortra-goanywhere-clop-ransomware/

[3]https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[4]https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/three-new-mandates-for-capturing-a-digital-transformations-full-value

[5]https://www.forbes.com/sites/forbesfinancecouncil/2023/06/15/digital-transformation-in-finance-how-companies-can-boost-resiliency/

Onymos