rewind

THE SAAS RESILIENCE PLATFORM

Even the best security teams still lose data.

Eight real data loss and ransomware incidents, and the recovery gap behind every one.

The organizations in this report aren't hypothetical. Every incident here happened to real companies, inside real SaaS and cloud platforms. And in every case, the difference between a bad week and a business-ending event came down to one thing: whether recovery was already built in before the attack started.

INSIDE THIS REPORT

- Ransomware inside the project tracker
- A server breached twice in one year
- Source code and cloud keys stolen, then sold
- 700 companies exposed through one stolen token
- $22M ransom paid, data leaked anyway

The pattern keeps repeating: the platform's own security never stopped the attacker or accident. What differentiated hours of downtime versus permanent data loss was one thing: backup and recovery living outside the compromised system. But first, what these gaps are costing everyone.

73%	29%	$9K	100%
of orgs say SaaS outages hit delivery timelines	have a defined recovery time objective for SaaS	estimated cost of downtime, per minute	lost revenue to an outage in the past year

Sources: Rewind SaaS Resilience Report, Q4 2025; Splunk, "The Hidden Costs of Downtime"; Cockroach Labs, "The State of Resilience 2025"

1

A global energy and industrial conglomerate: ransomware breaches the project tracker

WHAT HAPPENED

Attackers gained access to the company's project-tracking platform, an instance thought to be walled off from its core network. They moved through it undetected long enough to copy tickets, configurations, and integrations before triggering a ransomware demand.

WHAT IT COST

40GB of exfiltrated data, including more than 400,000 rows of user data, and a six-figure ransom demand designed to generate headlines as much as payment.

WHAT WOULD'VE STOPPED IT

A backup stored outside that instance, with the ability to restore to a clean point in time before the compromise. When recovery doesn't depend on the compromised system, a ransom demand has no leverage.

2

A multinational telecommunications provider: an exposed server breached twice in one year

WHAT HAPPENED

Attackers found an internet-facing project-tracking server that was misconfigured, then returned twice in the same year. The second time, they moved over 100GB of data in less than half a day using credentials stolen in the first pass.

WHAT IT COST

Invoices, employee records, customer databases, and internal network diagrams, exposed across two separate incidents the company didn't fully contain the first time.

WHAT WOULD'VE STOPPED IT

Independent monitoring and backup isolated from the exposed server. The second intrusion succeeded because recovery and cleanup after the first attack weren't independent of the same compromised environment.

3

A Fortune 500 professional services and IT consulting firm: source code and cloud keys stolen

WHAT HAPPENED

A threat actor gained access to internal development systems and exfiltrated source code alongside live infrastructure credentials, then offered the data for sale on a criminal marketplace.

WHAT IT COST

35GB of data, including SSH and RSA keys and cloud access tokens: the kind of credentials that can be used to move laterally into client environments long after the original breach is "resolved."

WHAT WOULD'VE STOPPED IT

Credentials and secrets kept out of the same backup and storage path as source code, plus a recovery plan that starts with rotating every exposed key immediately, not after forensics finishes weeks later.

4

Customers of a major cloud data warehouse provider: 165 accounts compromised, no MFA required

WHAT HAPPENED

Attackers used stolen credentials, most originally harvested by unrelated malware years earlier, to log into roughly 165 corporate accounts that hadn't enabled multi-factor authentication.

WHAT IT COST

Hundreds of millions of records across retailers, financial institutions, and consumer platforms, all through valid logins the platform itself never flagged as suspicious.

WHAT WOULD'VE STOPPED IT

This is the Shared Responsibility Model in its purest form. The platform secured its own infrastructure exactly as promised. The customers who got breached were the ones who hadn't enforced their own access controls or kept an independent backup of their own data inside it.

5

A CRM integration used by hundreds of enterprises: one stolen token, 700 companies exposed

WHAT HAPPENED

Attackers stole OAuth tokens from a single connected app, then used that trusted, already-authenticated connection to quietly query and export data from every organization that had installed it.

WHAT IT COST

More than 700 organizations affected, including companies whose entire business is cybersecurity, all through one integration none of them wrote or controlled.

WHAT WOULD'VE STOPPED IT

Independent monitoring of what your own CRM data does, and a backup of it that doesn't rely on the integration itself. A platform can vet its marketplace all it wants; it can't vouch for what a trusted app does once it's inside your account.

6

A major healthcare claims processing platform: a ransom paid, and the crisis didn't end

WHAT HAPPENED

A ransomware group encrypted core systems used to process insurance claims across thousands of providers, then threatened to leak the underlying data unless paid.

WHAT IT COST

$22 million in ransom, paid within days, on top of what became one of the most expensive breaches in the sector's history. The data leaked anyway in a second extortion attempt months later.

WHAT WOULD'VE STOPPED IT

A tested, independent recovery process that didn't depend on the attacker keeping their word. Paying a ransom is a negotiation with a criminal, not a recovery plan.

7

A mid-sized European services company: the ransom was paid, the company still collapsed

WHAT HAPPENED

A ransomware group encrypted the company's systems and exfiltrated a portion of its data, then demanded payment with a countdown timer and leak threats.

WHAT IT COST

A six-figure ransom, paid in cryptocurrency. The company still collapsed within the year, cutting its workforce by more than 95 percent.

WHAT WOULD'VE STOPPED IT

The ransom bought time, not survival. A recovery plan that didn't depend on the ransom payment working would have gotten the business back to operating in days instead of gambling the company's future on an attacker's promise.

8

A widely used education SaaS platform: paid once, breached again weeks later

WHAT HAPPENED

Attackers breached a learning management platform used by thousands of schools, and the vendor negotiated a payment to make the incident go away. Weeks later, the same attackers returned and breached it again.

WHAT IT COST

275 million records across roughly 9,000 institutions: one of the largest breaches recorded in the education sector, doubled by a second incident that happened because the first one was never truly closed.

WHAT WOULD'VE STOPPED IT

A recovery plan that closes the door completely, not one that assumes a paid attacker won't come back. Independent backup and hardened access controls after an incident matter as much as the response to the incident itself.

THE PATTERN

The pattern, and what resilience actually looks like

Eight different platforms. Eight different attack methods. The same failure every time: recovery depended on something the organization didn't fully control, whether that was an attacker's word, a vendor's infrastructure, or a single unmonitored integration. None of these companies lacked security budgets. Most had significant security teams. What none of them had, in the moment it mattered, was a recovery path that lived independently of the system that failed.

WHAT DOING IT RIGHT LOOKS LIKE

Compare that to what happened to a pension fund managing more than $135 billion in retirement savings. A cloud provisioning error deleted its entire cloud environment: every account, every service, gone in an instant. Not an attack, just a mistake. But because the organization kept a backup of that environment with an independent third party, outside the cloud platform itself, it restored everything. No ransom. No data loss. About two weeks of disruption instead of a business-ending event.

That's the difference backup makes when it's built in before the incident, not scrambled together after it. Under the Shared Responsibility Model, your SaaS and cloud vendors secure their platforms. They don't own recovery of what's inside your account, and neither does an attacker you've already paid.

It's also increasingly not optional. Frameworks like SOC 2, HIPAA, and ISO/IEC 27001, as well as emerging regulations like DORA all expect organizations to demonstrate an independent, tested recovery capability, not just a security policy. "We have a security team" is not the same answer as "we can restore this system ourselves, on our timeline, without needing the vendor or the attacker to cooperate."

Rewind backs up and recovers the SaaS data and dev tools your business runs on, independent of the platform, the vendor, and anyone trying to hold your data hostage.

SOC 2 Type II · ISO/IEC 27001:2022 · CSTAR Level 1 · 25,000+ organizations worldwide · 7+ PB backed up

Talk to Rewind about your recovery plan