6 Reasons to Protect Your SaaS Data

veeam

SaaS: Powering Today's Businesses

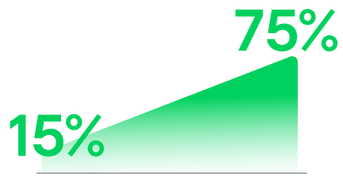
Software as a Service (SaaS) applications are the engine of modern business. From email and file sharing to customer data and finance, they keep teams moving fast and staying connected. They're flexible, cost-efficient, and scalable — and that's exactly why businesses have embraced them so quickly.

But here's the catch: SaaS application data isn't as safe as you think.

Too many organizations assume their SaaS provider has their back when it comes to data protection. The reality? Most platforms offer short-term retention and basic recovery tools that can't keep up with the speed and scale of today's threats. There's little protection against accidental deletion, ransomware, sync errors, or insider mishaps. And when it comes to meeting regulatory requirements, you're expected to figure that out on your own.

This is the shared responsibility model in practice. The provider ensures uptime and service availability. You handle the data itself — how it's secured, how long it's kept, how quickly it can be recovered.

As your systems expand across cloud apps, hybrid infrastructure, and distributed teams, that responsibility becomes harder to manage and more critical to get right. Small gaps in coverage turn into costly problems. Missed backups, delayed recoveries, and noncompliant retention policies can result in real damage — financially, operationally, and reputationally.



Right now, only 15% of enterprises view SaaS data backup as a top priority. That's expected to jump to 75% by 2028.

The shift is coming, but waiting isn't a strategy.

This e-book is built to help you get ahead of the curve. You'll learn exactly where the common gaps are, why native tools fall short, and what a modern, resilient SaaS data protection strategy actually looks like.

If your organization relies on SaaS to run key parts of the business, this isn't just helpful insight. It's essential planning.

Why Do SaaS Applications Need Data Protection?

1. Human Error & Accidental Deletion

SaaS platforms are essential to how businesses operate, but most teams underestimate how easy it is to lose important data. A simple mistake — like deleting the wrong file, misconfiguring a sync, or overwriting a shared record — can remove critical information from the system instantly. Many assume recovery is just a few clicks away, but that's rarely the case.

Most platforms (Microsoft 365, Entra ID, Salesforce) rely on built-in recycle bins with short retention periods and limited scope. Once that time is up, or if the data bypasses the recycle bin entirely, recovery becomes impossible. In many cases, the data you need isn't even covered — certain data types may never make it to the recycle bin at all. By the time you notice something is missing, it's often already out of reach.

These platforms are built for performance and collaboration, not long-term protection. And as organizations grow more dependent on SaaS for core business functions, these gaps become harder to ignore. One accidental deletion shouldn't derail a project, delay an audit, or disrupt a customer relationship.

2. Legal, Compliance, and Regulatory Risks

Regulations like GDPR, HIPAA, and NIS2 aren't just checkboxes — they come with real consequences. We're talking major fines, legal headaches, and damage to your brand if your data isn't stored, retained, or recovered the way the law requires.

As these frameworks get tighter and more global, relying solely on built-in protections puts your business at risk. And it's not just about ticking compliance boxes — it's about having full control when it matters most.

In 2024, the pressure intensified. Cyber-attackers got smarter, natural disasters tested infrastructure, and new regulations like NIS2 raised the bar. Now, as we push into 2025, attackers are using ransomware as a smokescreen while they silently exfiltrate or corrupt your data, while AI is adding speed and complexity to the equation.

Staying compliant — and staying in control — requires more than good intentions. It takes a real strategy, and the right tools to back it up.

3. The High Cost of Data Loss

Data loss doesn't just hit IT — it hits your entire business. It drains budgets, derails plans, and shakes customer confidence. Fines alone can climb into the millions, but that's just the start. Recovery efforts pull teams off mission-critical work, legal costs spike, and productivity stalls. Meanwhile, customers get frustrated, deals fall through, and competitors don't hesitate to fill the gap.

In today's fast-paced market, even one data incident can throw a company off course. Momentum is lost, priorities shift to damage control, and what started as a small error becomes a costly crisis. Too often, businesses underestimate how fast things can spiral. They treat data loss like an IT issue… until it disrupts revenue, reputation, and relationships.

Here's the truth: data is at the center of everything. Operations, customer experience, compliance, growth — it all depends on it. Lose control of your data, and you're handing over control of your business. And most of the time? It didn't have to happen.

4. Internal Security Threats

Internal threats are some of the most underestimated risks out there, and some of the most damaging. Employees, contractors, and vendors with access to sensitive systems can expose data, whether by mistake or on purpose. A misconfigured permission, a careless file share, or a malicious deletion can go unnoticed until the damage is done.

Hybrid work has only raised the stakes. With teams spread out and systems more open than ever, oversight is tougher, and internal threats can slip past traditional defenses. These aren't headline-making attacks from the outside, but rather quiet breaches from within. By the time you catch them, critical data may already be gone.

This isn't a rare exception. It's happening across industries, across teams, and across departments. And the fallout is serious — broken trust, stalled workflows, compliance failures, and costly investigations.

Internal threats aren't a "maybe," but a constant, inevitable concern. The real question is: will you have the visibility, the control, and the recovery plan to deal with it before it becomes a full-blown crisis?

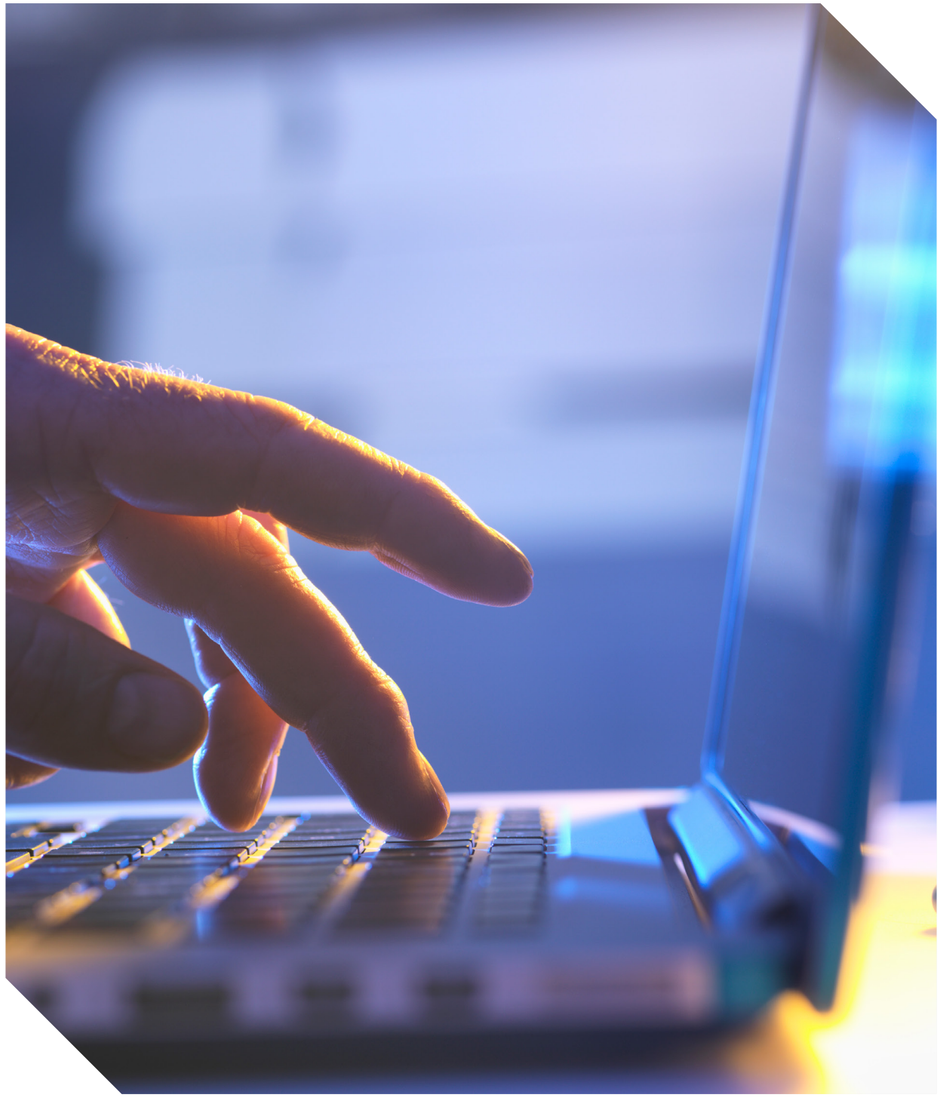
5. Cyberthreats

Cyberattacks are getting smarter and harder to stop. Ransomware has moved far beyond simple file encryption. Today's attacks often involve data theft, sabotage, and multi-step extortion tactics designed to overwhelm defenses and stall response teams. Phishing, privilege abuse, and stealthy malware are often just the beginning.

The financial hit can be massive. In 2024, the average ransom payment in Q4 alone was over half a million USD. But that figure doesn't reflect the full cost — lost revenue, legal action, operational downtime, and damage to brand reputation often do more harm in the long run. Regulatory frameworks like GDPR and NIS2 raise the stakes further, requiring companies to show that their data was protected before, during, and after an attack.

With hybrid infrastructure, remote teams, and a growing number of access points, attackers have more opportunities than ever. Defenders have to cover more ground with the same — or fewer — resources. AI-powered threats and more sophisticated social engineering are adding even more pressure to already stretched IT and security teams.

Ransomware is no longer just a security issue. It's a business risk, and it demands a modern, layered strategy to match its complexity. Organizations need to be faster, smarter, and fully equipped to respond.



6. Ensuring Business Continuity

Disruptions come in many forms — ransomware, outages, natural disasters — and when they hit, the clock starts ticking. Most teams aren't set up to recover quickly enough. According to Gartner analysts, ransomware recovery often drags on for weeks. That kind of delay takes a toll across the board.

Downtime cuts into revenue, frustrates customers, and drains internal resources. In sectors like healthcare, finance, and government, where every minute counts, the cost can escalate fast. Customers expect availability. When systems go dark, patience wears thin, and brand trust takes a hit. In complex environments, a single failure often affects multiple systems, partners, and end users. Without a reliable plan in place, small problems grow, and recovery becomes harder with every passing hour.

All together? Recovery speed isn't just about getting systems back online. It's about protecting the work your teams have built and the trust your customers expect, while every hour your SaaS data is compromised lost chips away at both.

So, the question becomes: is that a risk worth taking?

The Role of Third-Party Solutions in Data Protection

SaaS providers weren't built with full-scale data protection in mind. Their native tools cover the basics, but that's where it ends. Backup schedules are rigid, retention is short, and recovery options are limited. Critical features — like granular restores, extended retention, and compliance-ready reporting — simply aren't part of the package.

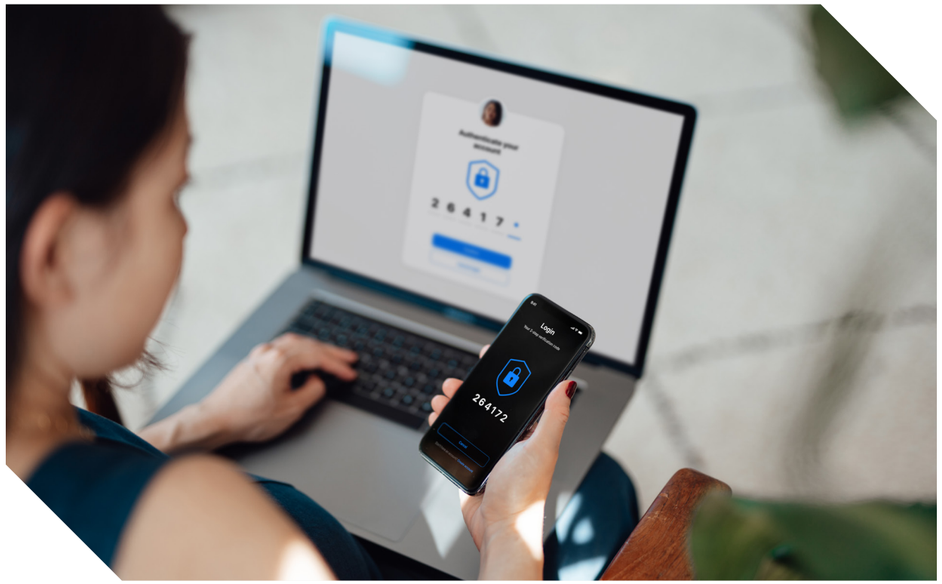
As environments grow more complex, these limitations create more risk. Teams are left stitching together workarounds, adding cost and complexity without solving the underlying problem. Visibility is limited. Flexibility is lacking. And when something breaks, recovery is often slow, incomplete, or impossible.

SaaS platforms are essential to how businesses operate — but default protections weren't designed for long-term resilience. Without purpose-built backup and recovery in place, businesses are managing critical risk with tools that fall short where it matters most.

The question is simple: if this is the data your business runs on, are the built-in protections really enough to protect it?

SaaS Data Protection in Action

More organizations are recognizing the gap in SaaS data protection — and they're acting on it. By 2028, 90% of companies expect embedded security in a SaaS data protection platform. The shift is already underway. Forward-looking teams are moving beyond native tools and adopting SaaS data protection solutions, unified platforms, and hybrid recovery strategies that cover cloud, SaaS, and on-prem environments.



They're choosing solutions with the flexibility and control they need: immutable backups, point-in-time recovery, long-term retention, and built-in threat detection. These aren't bonus features. They're the foundation of a serious data protection strategy.

Meanwhile, the risks keep growing. SaaS platforms run everything from sales to finance to collaboration. When something breaks — whether through error, attack, or outage — business stops. And for companies still relying on default settings, recovery is often limited, slow, or impossible.

Limited retention and rigid recovery don't hold up under real-world pressure. Businesses need protection that scales with their data, keeps them compliant, and moves fast when every second counts.

Recognizing the problem is step one. Now it's time to put the right solution in place.

What Does Modern SaaS Data Resilience Look Like?

The way businesses manage and protect data has changed. SaaS applications, hybrid infrastructure, and remote teams have created a new level of complexity. Cyberthreats are evolving quickly. Compliance standards are getting stricter. And too many organizations are still leaning on outdated tools or built-in platform settings that simply weren't built for what today demands.

Continue with 6 Essential Traits of Modern SaaS Data Resilience, which lays out exactly what today's organizations need to stay protected, compliant, and in control. Inside, you'll discover how leading teams are moving to cloud-native solutions that simplify operations while strengthening security.

- Eliminate recovery delays with fast, precise, policy-driven automation
- Centralize protection across SaaS, cloud, and on-prem workloads
- Strengthen compliance and security with built-in controls and real-time visibility

If you're still managing risk with a patchwork of aging tools or assumptions about what's covered, this guide will help you close the gaps.

→ Download the e-book and get ahead of what's next.

Additional Resources:

- → 7 Critical Reasons for Microsoft 365 Backup
- → 6 Reasons for Microsoft Entra ID Backup
- → Key Scenarios for Safeguarding Salesforce Data

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it.

Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data freedom, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 74% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam.

Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

→ **Learn more: veeam.com**