keepit

Key takeaways

SaaS data security: Risks, threats, and resilience

We're at a critical juncture for data security; the pressure to innovate with AI and manage SaaS complexity is redefining what it means to protect data. What's needed now is data security as a control — direct, data-centric protections that govern access, usage, and lifecycle. Organizations need to rethink their approach to data, which includes understanding the risks, mitigating the threats, and ensuring resilience.

This was the key focus of a recent Keepit webinar, where guest speaker Heidi Shey, Principal Analyst at Forrester Research, broke down the key components of a data-centric security strategy for SaaS environments and discussed practical next steps to adopt to both the knowns and the unknowns organizations are facing.

Three important steps to strengthen your security posture

Step 1: Define what to protect

Rethink what "sensitive data" really means and classify the full spectrum of data your organization relies on. Start with the three Ps (PII, PHI, PCI) and intellectual property — but go further. Every organization has corporate data of value (CDV):

- Chat and collaboration data
- IoT and sensor streams
- API keys, credentials, and developer secrets
- AI models
- SaaS data — and backups

Step 2: Identify the risks to mitigate

Understand the three dimensions of risk when planning for which risks to mitigate. Risk isn't just to your data, it also comes from and in the data:

- To the data: ransomware, insider threats, SaaS misconfigurations, failed backups
- From the data: privacy violations, unethical use, non-compliance
- In the data: stale, duplicated, or incomplete information that fuels bad decisions or AI bias

Step 3: Select data security capabilities and controls

Map controls to the right risks. No tool solves every risk — so you need to align controls purposefully.

Most importantly, consider how to secure your SaaS environments. SaaS applications have certain controls built in, but the shared responsibility model adds further complexity — not all the responsibility is on the SaaS provider, so you need to balance native versus third-party controls. You'll need to enlist the help of specialist vendors to fill the gaps of these environments when it comes to data security.

Resilience requires strategy, not hope:
Three checkpoints to improve resilience

1. Align with your vendors on the following resilience requirements:	
Improved data classification	☐
Integration with data governance	☐
Visibility into machine/API data flows	☐
Controls for AI prompts, outputs, and training	☐
Vendor readiness for post-quantum migration and agility	☐

2. Security isn't a solo act. Expand your stakeholder group to include these stakeholders:	
Data stakeholders	☐
Product owners	☐
Data science and analytics leads	☐
AI councils and compliance boards	☐

3. Ask the question: Does this solution introduce new risk? Risk is multifold and consists of:	
Technology risks	☐
Regulatory risks	☐
Operational risks	☐

"We are at this turning point, so use it as an opportunity to take a leap forward with your data security program to make bigger, beautiful things happen for your organization."

Heidi Shey, Principal Analyst, Forrester.

Data governance report

Read our data governance report for more insight into how to best classify, protect, and recover your data so you can ensure operational continuity.

Download now

Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on Linkedin