SPONSORED CONTENT | WHITE PAPER

Market Pulse

Can **data protection** keep pace with the shifting landscape?

Enterprise disaster recovery strategies crafted for on-premises IT infrastructure are struggling to keep up with growing reliance on cloud applications and the rollout of generative artificial intelligence (genAI) applications.

CSO

SPONSORED BY keepit®

Market Pulse

In a recent Foundry survey of 107 IT decision-makers at companies with more than 1,000 global employees, a large majority of the participating organizations indicated that they believe that their financial systems are relatively well covered by data protection strategies but that other key transactional systems and custom applications are less protected.

Increasingly, there is a critical security component to backup and recovery, along with a compliance component, that is becoming more important with regulatory scrutiny of disaster recovery preparedness, rapid implementation of AI and machine learning (ML), and the move of data and processes to the cloud.

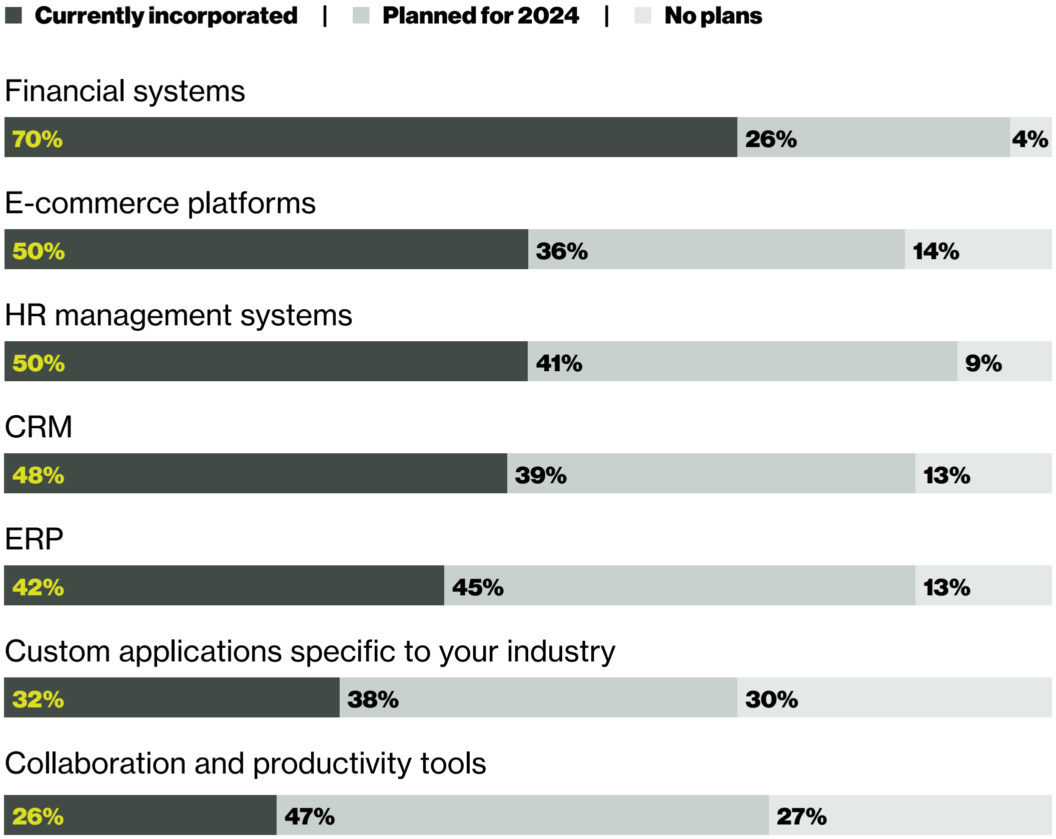
Of those surveyed, 70% said their financial applications – whether software as a service (SaaS) or on-site – are incorporated within data protection strategies and 26% said that that will happen in 2024.

Half said their e-commerce and human resources management systems are covered by those strategies, with many others hoping to catch up this year. However, critical transaction-based systems, custom applications, and collaboration and productivity tools remain behind (see Figure 1).

One decision-maker participating in a recent roundtable hosted by Keepit lamented that many of today's challenges were largely sorted out 10 to 15 years ago, but "Then we went to cloud, and it seems like a lot of lessons around information governance, managing data, and what you do with data got forgotten, and now we're starting all over again."

[**70%** of those surveyed said their **financial applications** are incorporated within **data protection strategies.**]

Figure 1 | Which SaaS or enterprise applications do you currently use in or plan to incorporate into your data protection strategy in 2024?



SOURCE: FOUNDRY

Strategic gaps

Just half of those surveyed have brought cloud-stored data of SaaS under their disaster recovery plans, and another 40% said they are planning to do so.

Most respondents recognize the vulnerabilities in their current data protection strategies. They expect to be able to extend those strategies to cover most applications in the coming year. However, for some, those aspirations are likely to be hampered by conflicting demands for IT resources, organizational resistance to change, and the need to implement new initiatives — such as governance of the data used by large language models (LLMs).

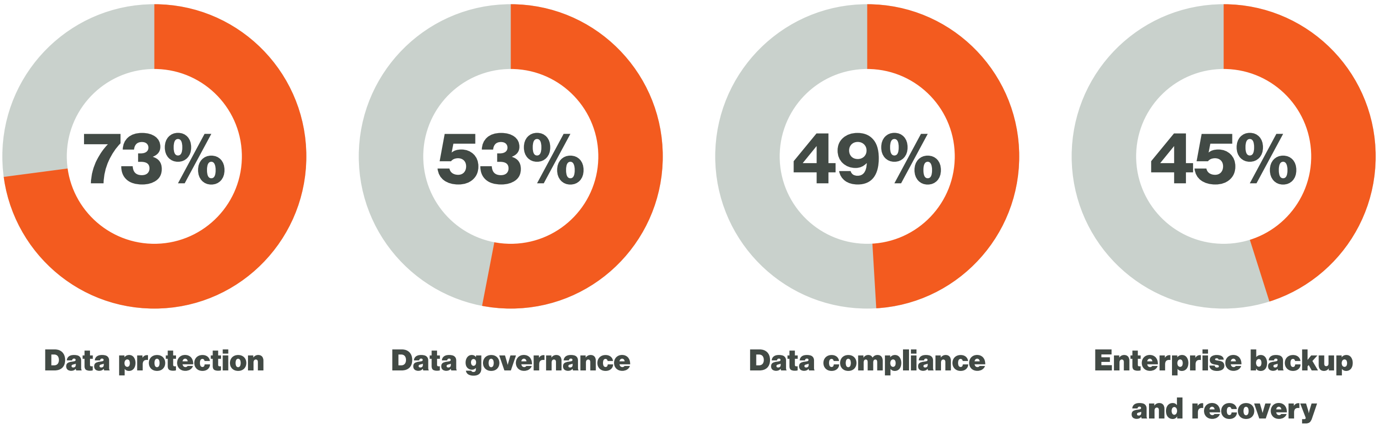
Virtually all the respondents are prioritizing AI data protection. Just over half have already determined how to move forward, with the rest saying that it is currently under consideration. A significant majority indicated that their current state of data protection is a limiting factor for exploring or expanding use cases for genAI technologies.

Compliance and future-proofing challenges

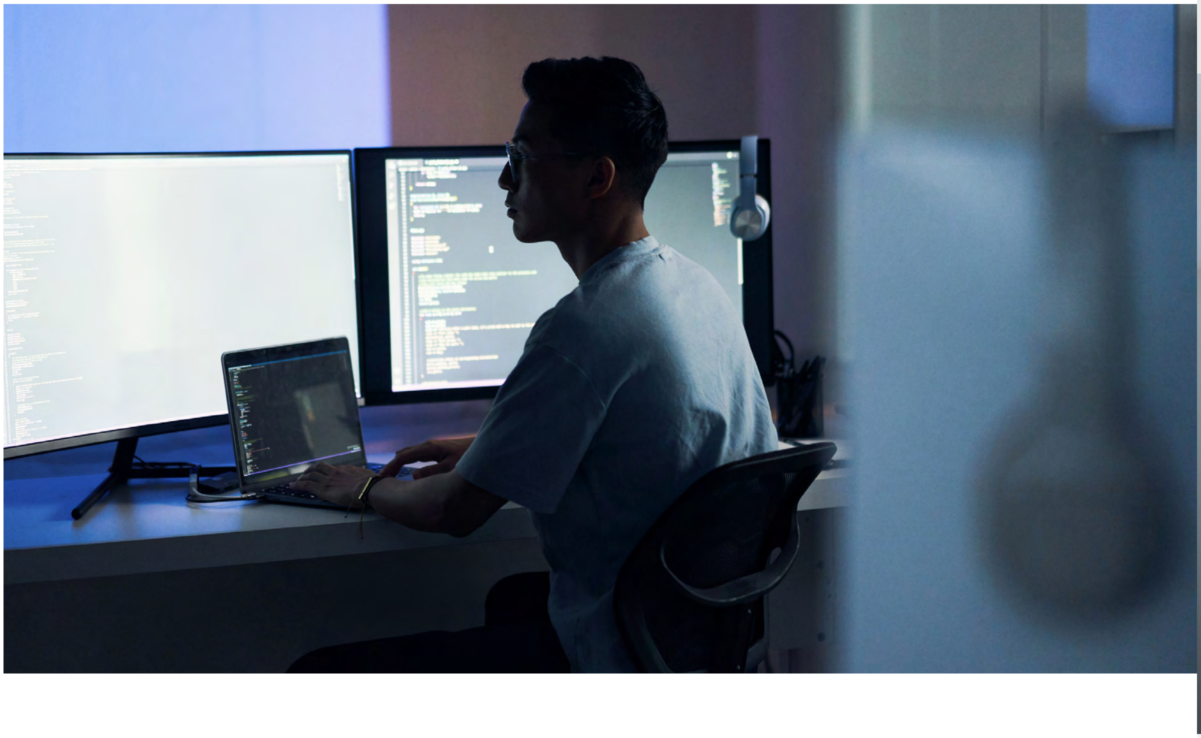
Data protection is the main challenge or need to address in 2024, according to 73% of the survey respondents (see Figure 2). Asked to select all that apply from a list of common issues, many also chose data governance (53%), data compliance (49%), and enterprise backup and recovery (45%).

Regulatory agencies, such as the U.S. Securities and Exchange Commission (SEC), have responded with mandates for managing cyberrisks, requirements for

Figure 2 | Challenges or needs to address in data protection strategy for 2024



SOURCE: FOUNDRY



cybersecurity resilience, and new reporting obligations. In the EU, financial services companies face a January 2025 deadline for compliance with the Digital Operational Resiliency Act (DORA) and uncertainty about how member nations will implement the Network and Information Security 2 directive, which aims to modernize and boost cybersecurity throughout the region.

What makes this particularly challenging, according to one-on-one chief information security officer (CISO) interviews commissioned by Keepit, is the difficulty of managing multiple security vendors and the gaps that occur due to the use of disparate solutions. Meanwhile, cybersecurity risks, most notably ransomware assaults, where organized crime and state-sponsored gangs have raised the ante considerably, are continuing relatively unabated.

One roundtable participant said his organization had experienced five major cyberattacks over the course of the previous year, resulting in shutdowns of payment processing, health insurance, and a joint venture. “We’re in the process right now of redrafting our whole cyberresponse plan based on our learnings,” he said.

Staying on course against the headwinds

The survey and interviews with decision-makers indicate a strong interest in a defensible security strategy that designs, builds, operates, and defends an infrastructure while continuously applying both threat modeling and analysis.

That requires a common data governance framework across the organization and all IT assets, but achieving that is not a simple matter. For example, less than one-third of the survey respondents said their data protection vendors cover all or most of their applications and just 58% of applications, on average, are protected.

Further complicating such a framework is the reality that SaaS and cloud vendors employ a shared-responsibility model that often places the onus on customers to ensure that data is safe. IT departments, therefore, cannot rely solely on their cloud vendors to preserve data and thus need to adhere to the legacy 3-2-1 backup rule, which requires multiple copies of backup data on many different devices and in separate locations.

True backup protection requires a logical infrastructure separate from the primary data, but many cloud-based services back up customer data to the same cloud in which production data is held, creating potential risk if the vendor is attacked. ◆

Learn how to protect all your key SaaS applications with Keepit in a single vendor-independent platform.

© 2024 IDG Communications, Inc.