Microsoft Security

# Data Loss Prevention: From on-premises to cloud

How solutions have evolved and why you should too

# Forward

*Rudra Mitra*
**CVP, Microsoft data security and privacy**

As work has become increasingly digital, data landscapes have naturally grown more complex. With this comes an increased need to help organizations secure their data across both cloud and applications while at the same time quickly adapting their data security practices.

At Microsoft, we take a similar approach – evolve our security practices with the ever-changing landscape. As the Corporate Vice President for Microsoft data security and privacy, I work hand-in-hand with other leaders across the company to make sure that we are addressing our data security needs while also continuing to build employee trust, which is our first line of defense. My team works hard to create solutions that empower our customers to do the same. Given our unique position, we are committed to sharing our learning with customers and providing solutions that allow them to take a holistic approach to protecting their most important asset – their data.

We recognize that it is a challenge to prevent data from getting into the wrong hands in this growing digital landscape, and in my conversations with customers, I have learned that based on where organizations are in their journey, they need different things from Microsoft. Some are looking to us to provide guidance, others ask for tools that can help them get started easily, and some need sophisticated solutions that can meet the complexity.

Research shows that among the organizations that use traditional data loss prevention solutions, (DLP) 73% are concerned with data transformation difficulties, and more than half cite enabling productivity is a challenge. At Microsoft we continue to empower organizations through their digital transformations so they can face the data security challenges of this modern workplace head on while maintaining productivity.

For this report, we spoke to hundreds of security leaders around the United States to learn the very real needs and very real risks they face and how they can best be supported. This report discusses a continuum for the evolution of DLP solutions – from on-premises to the cloud. We learned that organizations who do use cloud DLP solutions are twice as likely to say - that cloud DLP solutions – are not only easier to scale, but more importantly help balance data protection and employee productivity. And we also discuss the challenges that organizations face and why despite these challenges, adopting a cloud-based DLP solution can bring cost savings, scalability, and empower employees to be productive.

# 00 Executive summary

Today working together means working in the cloud across the globe with flexible work arrangements that include hybrid and remote work. No longer being restricted to four walls of an organization provides employees flexibility to collaborate and uphold productivity across the digital estate. With this adaptability comes an even greater need for data security and the right data loss prevention (DLP) solution.

The purpose of this Microsoft-commissioned study was to delve into the data security landscape to find out how companies are managing and perceiving success of their DLP solutions. The goal of the study was to 1) uncover the top priorities and challenges facing organizations, 2) understand the evolution of firms' DLP solutions as they address today's shifting digital landscape, and 3) discover what barriers stand in the way of firms' adopting cloud DLP solutions.

This paper details the survey results of 307 DLP professionals and compliance decision makers from US-based companies to understand their current approach to DLP, perceptions of solution benefits and limitations, and barriers to cloud migration of DLP solutions.

**How do firms evolve their DLP solutions?**

What respondents revealed surprised us. Our research found that perceptions of success and confidence don't always align with reality. Respondents progress on a continuum—from on-premises DLP solutions toward the cloud—in states as they face (and address) barriers like uncertainty, cost, perceived complexity, impact to productivity, and employee education. We identified the role history plays in movement through this continuum and we created profiles about companies at each of the DLP states, landing on the ideal solution state.

We found that companies who are more proactive in their approach to DLP are better prepared to mitigate the impact on productivity. Companies in more evolved DLP states have strong focus on employee education and processes that better aligns with a holistic approach to DLP and data security.

The report tackles how organizations consider challenges as they adapt DLP solutions to meet their evolving needs. We feature recommended best practices for security leaders regardless of where they are in their own DLP journey and explain why leveraging a cloud-native DLP solution— delivered and managed in the cloud and already integrated as part of the cloud providers services and productivity suite offering—is beneficial to achieve the ideal state.

*"Data is not confined in a certain area. In today's environment, it's everywhere; someone's else's phone, tablet, data center, or SaaS application—because of that, you definitely see a lot more breaches happening."*

*VP, ISO, Financial Services*

# 01 Data protection is a shifting landscape

Data is everywhere. It's that simple. Today, working together means working in the cloud where many employees are empowered to collaborate across time zones, devices, platforms, and networks without having to step outside their homes. This flexibility generates more messaging, file sharing, and document uploading and downloading across the digital estate—making it imperative that data should be protected throughout its lifecycle.

Whether data is being created, processed, stored, shared, or destroyed there needs to be a system in place that protects data at each stage. Data by its very nature is ever changing. It can move back and forth between the different lifecycle stages and could be located in completely different data environments, such as on-premises and in the cloud. This hybrid nature of modern data compounds the data protection complexity. Furthermore, with people working in the cloud from so many locations and devices, organizations are forced to continuously perform the balancing act between the utmost security across an egress-prone data environment, without compromising productivity. So how does an organization know they are providing the best protection for their data?

We know a good data loss prevention (DLP) solution protects a company's data assets, aids regulatory compliance, and prevents sensitive data leakage. An effective approach to DLP also requires organizations to look at people, processes, and technology holistically as part of their data protection strategy.

According to Forrester, "today, data isn't only IP and regulated data such as personal data, cardholder data, and healthcare information, but also operational data, and data about your data, business processes, and more. The value derived from this data is what differentiates your firm's products and services, and it requires protection from both internal and external threats." [1]

**What is data loss prevention?**

For the purposes of this paper, (DLP) is defined as a strategy that uses a combination of people, processes, and technology to ensure that sensitive data is not lost, misused, or accessed by unauthorized users. DLP protects an organization's data against accidental or malicious sharing that could put the organization at risk. DLP solutions help control endpoint activities, filter data streams on corporate networks, and detect data in the cloud to protect data at rest, in motion, and in use.

*"The phrase DLP is like the phrase organic or artisan when you go shopping for bread or food. Most people don't know what it means."*

**Director, Technology Services**

The growing complexity of modern data environments, from on-premises to the cloud, makes DLP a focal point in overall data protection strategy for most organizations. How do IT professionals maintain high security, while balancing organizational demand for productivity? How do organizations ensure their solution best meets their needs? What pushes some toward differing beliefs about their data security maturity? We spoke with US-based organizations to find the answers to these questions and more.

**In this paper you will:**

- Learn how companies perceive success with their DLP solutions

- Uncover the top DLP priorities and challenges organizations face

- Understand how respondents are thinking about evolving their DLP solutions with the changing data environments

- Discover what barriers stand in the way of firms' adopting cloud DLP solutions

*"What you are trying to protect against is always changing. It's a moving target. It's always going to be evolving, changing, and flexible. What you are protecting and where it lives is only going to get more varied."*

*VP, Sr. Manager, IT, Financial Services*

How are companies thinking about data protection to address the ever-evolving risks? Our research found 70 percent of companies saw their DLP solution as a focal point of their data protection strategy. The story remained true across industries with both regulated and non-regulated companies indicating the impact of DLP on the firms.

*"We operate internationally and adhere to standards like GDPR in Europe. We focus on protecting our intellectual property, our designs, and our data. We also focus on protecting the standard stuff: personal data, HIPAA, and health data."*

*VP Cybersecurity, Manufacturing*

In addition, a majority of respondents (59 percent in *figure 01*) highly agreed their DLP solution should be part of a holistic approach to data protection strategy. This finding aligns with previous Microsoft research exploring the impact of insider risk 2 on data protection, where holistic strategies provided a greater level of protection for the company when coupled with a strong DLP program. These holistic strategies look to utilize not only technology solutions like DLP but also incorporate people, processes, and education into the overall approach.

Figure 01: Highly agree DLP should be part of a holistic approach

*The DLP program should be part of a holistic approach to data protection strategy*



**59%**

*"We take a much more holistic approach to DLP because very few times does somebody actually get in and steal your data. It's all of the other types of instances where data can move across the environment and place you at risk. We look at all of these things and manage it as a holistic DLP strategy."*

*CIO, Healthcare*
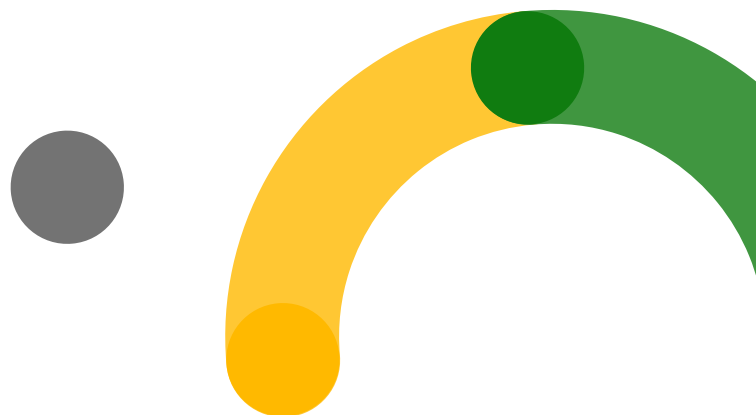
# What we learned

## Perception can be misleading

Respondents across different organizations, industries, and firm sizes seem to have high confidence and perceived success in their DLP programs with 8 in 10 self-reporting strong scores for their programs (*figure 02*). However, the established history of DLP within organizations might have created a false sense of security and the level of discomfort around DLP migration further backs this.

We found different approaches impact overall perceptions of success and confidence. Organizations who have migrated more fully to a cloud DLP approach report higher satisfaction and confidence with their programs compared to those who are still operating in more hybrid and on-premises data environments. Companies moving their data and DLP solutions toward the cloud know they will face more challenges, as opposed to remaining comfortable where they're at. They also know remaining static makes the organization more susceptible to internal or external threats. Evolution becomes necessary and inevitable.

*I think about this whenever we buy almost any solution these days. Is there a path to the cloud if we decide to go with the on-premises version of this? Is there an easy path that if we wanted to move this to the cloud, we could do that at some point in the future?*

*Sr. IT Manager, Financial Services*

**Figure 02: Confidence in and Success with DLP program**

*Have high level of confidence in their DLP program's protection against data loss* — 82%

*Highly rate the success of their organization's DLP program* — 80%
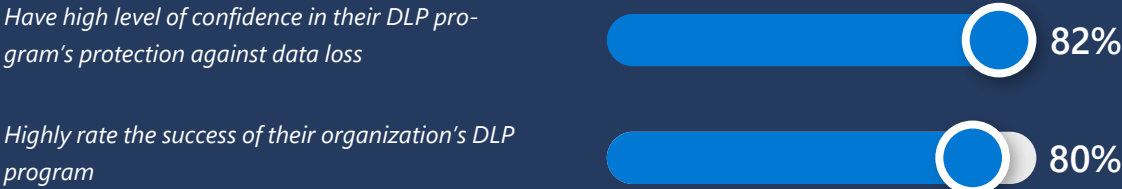
## Complexity and need for clarity

We found while most respondents claimed to understand their DLP solutions and approach, many struggled to articulate their style and best practices. Part of this could be because IT professionals across the board told us that working with traditional on-premises DLP solutions isn't easy; some respondents said they go as far as trying to ensure the employees staffed on the work are rotated so they don't burn out.

Add to that the impact of remote and hybrid work, migration of data and infrastructure into the cloud, and varying terminologies and departments involved with handling data protection—and it all quickly becomes complicated and taxing.

*"The threat landscape is ever changing."*

*Senior Manager, Data governance, Telecommunications*

While DLP has been around for decades, the recent upheavals in the work world require companies to evaluate their positions, adapt, and evolve. In *figure 03,* we found 40 percent of DLP professionals we surveyed strongly agreed there was a need for clarity around the best approach, with many more agreeing in general some clarity is needed in this area.

**Figure 03: High agreement of needed clarity**

*There is a lack of clarity in the DLP market around the best strategy for data loss prevention*



40%
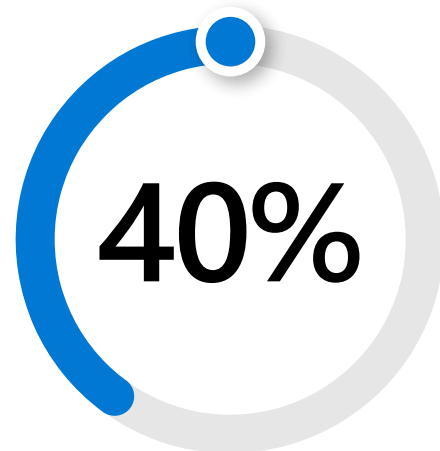
*"Usage is different, consumption is different. We're constantly looking at process. Where are my crown jewels."*

*Cybersecurity ISO, Financial Services*

## Progressing to the cloud
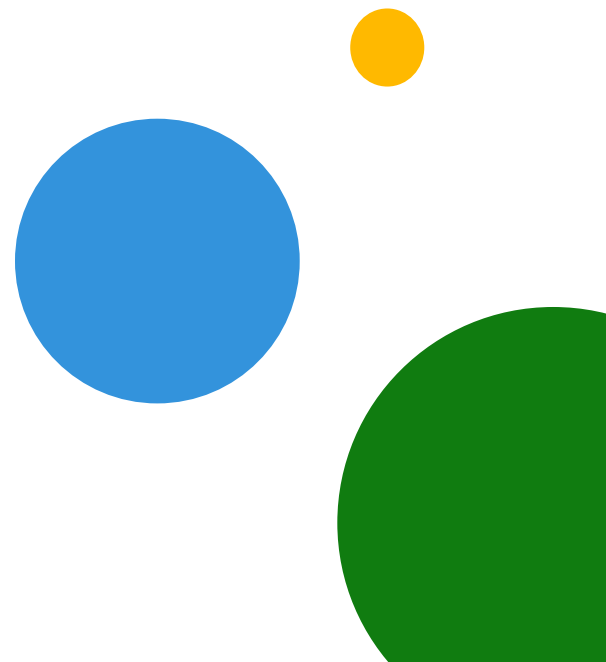
Despite their high level of confidence and success, most respondents are not content with their position and **aspire to continue to migrate their data to the cloud and adopt cloud DLP solutions**. Among those who are migrating or expecting to migrate their DLP solution, 60 percent envision moving all of their on-premises solutions to the cloud, while another 37 percent expect to move at least some of their remaining on-premises solution to the cloud (figure 04). This indicates a vast majority of DLP professionals expect to see change in the near future—indicating they know they must continue to evolve.

**Figure 04: Interest in migrating current on-prem DLP to cloud**

*Move ALL*
**60%**

*Move SOME*
**37%**

*NOT Moving*
**3%**
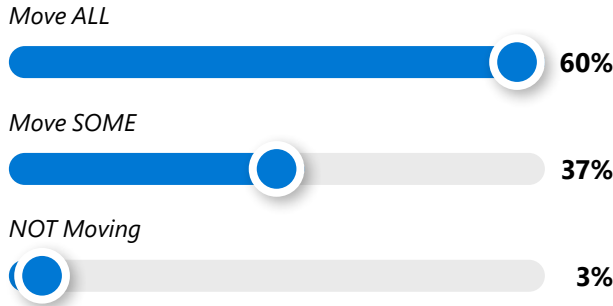
*"It's time to stop living in this legacy mindset that everything needs to be a physical thing in our four walls that we have to be able to touch and feel to feel safe."*

**Sr. IT Manager, Financial Services**

## DLP states

To understand the future of DLP, we looked at the evolution of where companies have been and where they are now when it comes to protecting their data.

Beyond the past state and future state of DLP, we found three fundamental states of DLP programs: on-premises–anchored, hybrid, and cloud-focused. Most organizations' DLP programs will fit into one of these three states; how they progress from one to the next, and why, is elemental to the evolution we will explore in this paper.

*"The only way that the higher ups were going to green light migrating to cloud is that we could say with certainty that we are going to be as secure - if not more secure - with this cloud deployment as we would on-premises."*

**Sr. IT Manager, Financial Services**

However, before we dive into what the DLP states are and the future progression of DLP solutions for organizations, it's important to understand where we came from. In the next section, we review the history of data loss to further understand the evolving nature of DLP.

# 02 Data exfiltration tactics since the 1980s

Organizations have coped with data loss for decades but traditional DLP solutions haven't necessarily evolved to keep up. We start by tracing DLP solutions back to the 1980s when success for data exfiltration was judged by the number of records stolen.

In the 1990s, email takes off but because it's so new, firms don't focus on security considerations. The internet welcomes eCommerce and the motivating concern is whether or not it's safe to share credit card details across the web. Identity theft isn't a new concept in the '90s but the internet facilitates its online growth into the new millennium.

The 2000s welcome the start of the mobile and cloud era—and also the blurring of boundaries— where a user's personal and work data begins coexisting on the same devices. IT departments lose control as employees acquire their own devices and insist on connecting to the corporate network, adding device loss and theft to the possible security risks to a company's data assets.

During the 2010s, the concept of DLP grows exponentially as cybersecurity professionals realize the challenging task of really understanding what data is leaving their networks. On-premises DLP solution providers scramble to retrofit their legacy frameworks and offerings to adapt to the cloud.

By 2020, some organizations are already evaluating hybrid and remote work models. COVID-19 accelerates flexible work arrangements as many employees flock to home offices and eventually cafes, airports, and even abroad—basically anywhere a Wi-Fi signal is available. Companies progress along cloud adoption states with different motivations seeking the right security solution.

*"Running an email server 20 years ago was something you could do ... now, you literally have no choice but to go [to the cloud] when you want to have a reasonable degree of security and protection because the complexity is mind-blowing."*

*CISO, Healthcare*

# Data loss is as old as computing

## 1980s

- In the '80s, success for data thieves measured by the number of records stolen

## 1990s

- The internet opens doors for eCommerce; concerns swirl around credit card security
- Firewalls become the standard tool to restrict traffic in and out of networks

## 2000s

- Blurring of personal and work boundaries on devices
- Malware evolves from realm of pranks to monetized economy and cybercrime

## 2010s

- Ransomware and insider risk incidents continue to rise
- Emergence of Bitcoin in 2010 provides an easy, untraceable method for receiving payment from victims

## 2020s

- Remote and hybrid work accelerates
- Employees log in from remote locations, adding to data security concerns

# Trends influencing DLP solutions

Today, we have more data than ever. It's moving in and out of an increasing number of end points. Employees are not only using email but also instant messaging applications, sharing sensitive content multiple times a day. The unstructured data generated by these productivity tools creates continuous data exfiltration risks that require dedicated focus to keep sensitive data safe and protected.

*"Today, data can be transmitted, copied, and placed in so many places, it can be hard to manage."*

**Cybersecurity Executive, Utility Service**

As organizations continue acclimating to hybrid and remote work arrangements, they're having to adapt their data protection strategy to cover a heterogenous device landscape as employees are using a wider range of devices in more locations outside the organizational boundaries.

As called out by Forrester, "The challenge is how to protect exabytes of data that's strewn across your global data centers, computer rooms, remote offices, laptops, desktops, and mobile devices as well as hosted by many different cloud providers—especially during the past two years where knowledge workers worked primarily from home." [3]

Many companies are still reporting security talent shortages. Some affirm they have jobs to fill but need data security training to be in place. We see this echoed in the insider risk research[4] where, "Finding reliable personnel you can trust to complete the job of insider risk detection and remediation is one of the challenges to running a successful insider risk management program."

Delving into the history and evolving nature of DLP allows us to now pivot and look toward where we are headed.

*"Nobody has enough staff. The staff you have doesn't have enough time to get trained on and be really good at everything. Security options are important on many levels. You can't afford to either cheap out on or not do well because being on defense, you've got to be on point 100 percent of the time."*

**Sr. IT Manager, Financial Services**

# 03 Is there a DLP ideal state?

When we look at the future direction of DLP solutions, our findings show organizations move in a progression toward a cloud-only DLP state on the solution continuum, as follows:

**Figure 05: DLP states**

**Hybrid**
Looking to push their program
forward but seem static
*(Mostly equal split)*

**On-premises–anchored**
Want to change their state
but may face greater obstacles
*40 percent cloud*
*60 percent on-premises*

**Cloud-focused**
Moving towards the ideal
cloud state
*60 percent cloud*
*40 percent on-premises*

**Past State**
*100 percent on-premises\**

\* This state is no longer the norm as users have progressed

**Future State**
*100 percent in the cloud*

In physics, we describe phases of change as states—such as solid, liquid, gas. We know under certain conditions, we can use the different states as needed for our purposes or to our advantage. Similarly, we see organizations fundamentally use a mixture of techniques to protect data assets. Each company could be at different points of the continuum, utilizing pieces of each state. However, the goal is to evolve into the final state of the continuum—cloud-only.

As expected, none of our respondents reported being in the on-premises–only past state. As mobile and cloud computing popularized in the new millennium, companies began progressing on the continuum and none of our respondents were truly cloud only... not yet at least.

*"The sheer amounts and volume of data that a DLP solution picks up on is massive and I can't scale that in a database on-premises."*

*CISO, Telecommunications*

According to a Forrester report, when respondents were asked about the technologies their firms planned to adopt in the next 12 months to manage their privacy program, of those that mentioned DLP, 25 percent said they'd implemented DLP but had no immediate plans to expand (aligns with the hybrid state we identified), 21 percent stated they were in the process of implementing DLP (like on-premises–anchored), and 18 percent had implemented and were expanding its DLP adoption (similarly aligned as the cloud-focused respondents in our study) [5].

# The DLP Continuum States

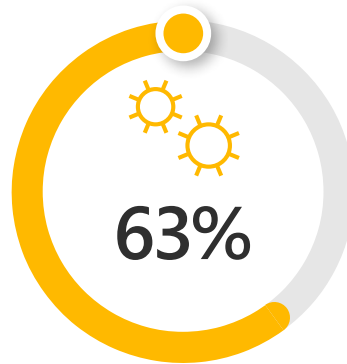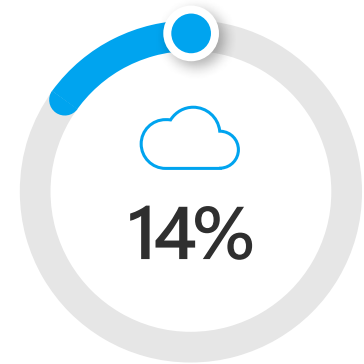| On-premises–anchored: where a firm's DLP solutions reside predominately on-premises with some elements in the cloud | Hybrid: where the DLP solutions exist in generally equal proportion on both on-premises and in the cloud; set toward a cloud-focused state | Cloud-focused: in which the organization has the majority of its data in the cloud and is predominantly using a cloud DLP solution |
|---|---|---|
| **24%** | **63%** | **14%** |
| On average, at least 60 percent of their data is on-premises (perhaps not by choice but due to cost or regulatory requirements) | A more balanced split between on-premises and cloud data | On average have at least 60 percent of their data in the cloud |
| Concerns about migrating to the cloud (either due to misconceptions or real difficulties related to larger amount of on-premises data, but know they need to make the leap) | Currently in the process of migrating. They want to move to the cloud but don't seem to be in a rush | Most likely to have migrated a DLP solution fully and are farthest along in their migration plans |
| Report a much greater level of challenge across most elements of their DLP program<br><br>Higher concerns about cost and policy recreation than other states | Overall DLP challenge perceptions similar to cloud-focused and in some areas lower<br><br>See biggest challenges around custom integrations | Lower level of challenge with their current DLP programs and clearer understanding<br><br>Are challenged with tracking users following policies |
| Continually look for their next DLP solution<br><br>*Seek innovation and help with data discovery and classification* | Evaluate new DLP solutions annually<br><br>*Seek improvements in scalability, flexibility, and accuracy* | Evaluate new DLP solutions at a slower rate (every 2 to 3 years)<br><br>*Looking to improve visibility into their data with their DLP program* |
| More focused on maintaining their infrastructure and managing device agents via on-premises DLP solutions<br><br>*Lowest level of perceived success and confidence in their DLP program* | Effort is often spent stitching together and managing their multiple DLP solutions to support their hybrid data environments | Look to DLP cloud solutions to provide security protection benefits that hybrid and on-premises–anchored firms must manage on their own<br><br>*Highest level of confidence and perceived success in their DLP program* |

While the majority of our survey respondents self-identified in the hybrid state, we heard about organizations in the process of fully migrating their DLP solutions to the cloud-only state. A small number of organizations might never be able to achieve the cloud-only state, due to industry regulations, compliance, or insurmountable challenges like cost. But based on this research we believe the cloud-only state is the ideal DLP approach for the majority of companies and progressing though the previous states is an inevitability in their futures.

**Assess yourself:** Based on our DLP states, where does your firm show up on the continuum?

*"What drove us to the cloud? All the good, new features that we wanted were not getting rolled out to on-premises. So, it's not like we had a choice. You want the good, new features, you had to move to the cloud."*

*CISO, Healthcare*

# 04 What challenges keep organizations from progressing to a new state?

If the continuum reveals a progression toward the ideal cloud-only state, are there attitudes or behaviors holding back organizations in the on-premises–anchored and hybrid states? For many respondents, the challenges they face help define their company's position on the DLP solution continuum.

## Are firms in the hybrid state comfortable?

Organizations in the hybrid state (where most companies sit) report a lower degree of challenge with their current DLP program compared to their on-premises–anchored counterparts and in some cases even the cloud-focused firms.

At first glance, this group appears to have a higher level of comfort with their DLP program. But 59 percent of the respondents in the hybrid state report a desire to move **all** of their DLP solution to the cloud and another 39 percent say they want to move at least some of their current on-premises solution to the cloud *(figure 06)*. This indicates a significant expectation to change their DLP state despite having lower levels of challenge with their current program.

**Figure 06: Among hybrid state - Interest in migrating current on-prem DLP to cloud DLP**
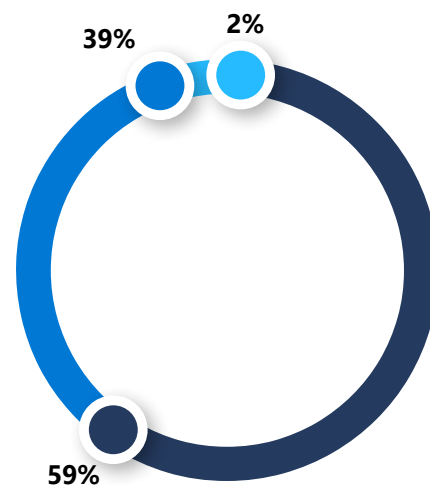


● Move ALL    ● Move SOME    ● NOT Moving

So is hybrid a comfortable state after all? Could the unknowns and perceived challenges about migration play a part in keeping firms in the hybrid state from making the leap? Or are the benefits of migration enough to drive organizations to evolve?

*"There is always the risk of the unknown ... It's very hard to compare on-premises to cloud."*

**Director, Technology Services**

## Challenges and barriers

To help us understand the key barriers keeping companies from moving forward on the continuum, we looked to the on-premises–anchored respondents. Within this group, we see a different narrative developing around caution, anxiety, and the unknown. Are these factors also preventing progress for hybrid and cloud-focused firms from moving to the final cloud-only DLP state?

*"Anything could happen where things could very quickly escape your grasp. It gets easier for that to happen and then harder for you to defend against it."*

**Sr. IT Manager, Financial Services**

## Discomfort with the unknown

We list this challenge first because it threads through all the others. It's important to clarify who is expressing discomfort about the unknown. We learned that C-suite executives called out the cost of the migration work. Meanwhile, IT administrators feel uneasy about the perceived heavy lifting involved, and IT managers might be hesitant to rock the boat by pushing something new when they've been using the same solutions for a long time. Apprehension around the unknown might arise from different areas and decision makers within an organization.

*"You can't do one or two things alone and be able to sleep at night."*

*VP IT, Financial Services*

This uncertainty is one reason some organizations don't pursue migration more aggressively. It may be a leader's discomfort that holds things up. Among respondents with on-premises–anchored DLP solutions, we see 6 in 10 cite apprehension around losing program ownership as a key barrier for movement (*figure 06.1*). Even among the other states, a good portion indicated uncertainty as a potential barrier to making the leap. The unknown risks of moving from one state to the next impact choices made by decision makers—where emotion can often drive big decisions.

*Figure 06.1* also shows that even when firms aren't satisfied with their current DLP solution, the perceived risk for migrating acts as a barrier—especially among the on-premises–anchored respondents.

**Figure 06.1: Agreement of the impact of fear towards migration**



**Barrier**

*Losing ownership of current DLP program to someone already qualified in the new DLP solution*

- 41%
- 48%
- 60%

**Attitude**

*I'm not content with my current solution but it's risky switching to a new DLP solution*

- 34%
- 28%
- 55%

● Cloud-focused   ● Hybrid   ● On-premises–anchored
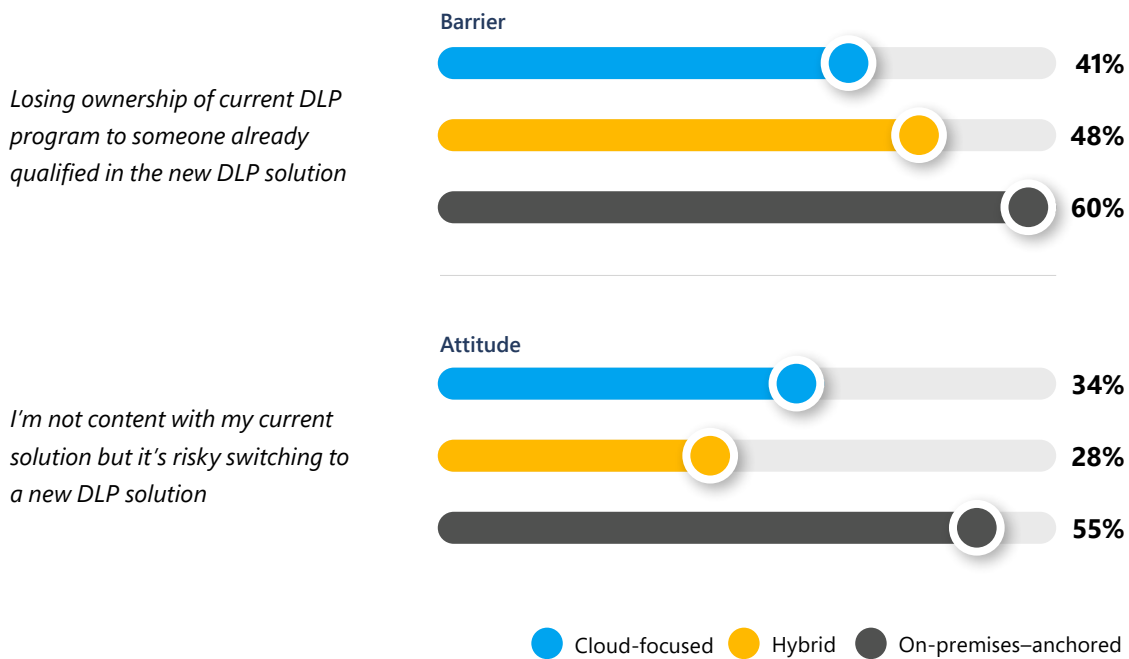
## Time and money

Financial considerations are a challenge for all organizations on their journey across the DLP solution continuum, with nearly 60 percent at a total level reporting this as a top barrier to migration. On-premises–anchored companies are even more likely to indicate financial considerations are impactful with 70 percent saying the initial cost of migration is a high-impact barrier *(figure 07)*.

**Figure 07: High agreement with cost and time challenges**

**Attitudes towards migration cost**

*Obtaining adequate funding for program operation is difficult*

- 40%
- 31%
- 50%

**High impact barriers to migration**

*Financial investment required to migrate initially*

- 54%
- 56%
- 70%

*Cost required for post-migration maintenance*

- 50%
- 57%
- 53%

*Time required to test and evaluate new DLP solution*

- 49%
- 57%
- 53%

● Cloud-focused  ● Hybrid  ● On-premises–anchored
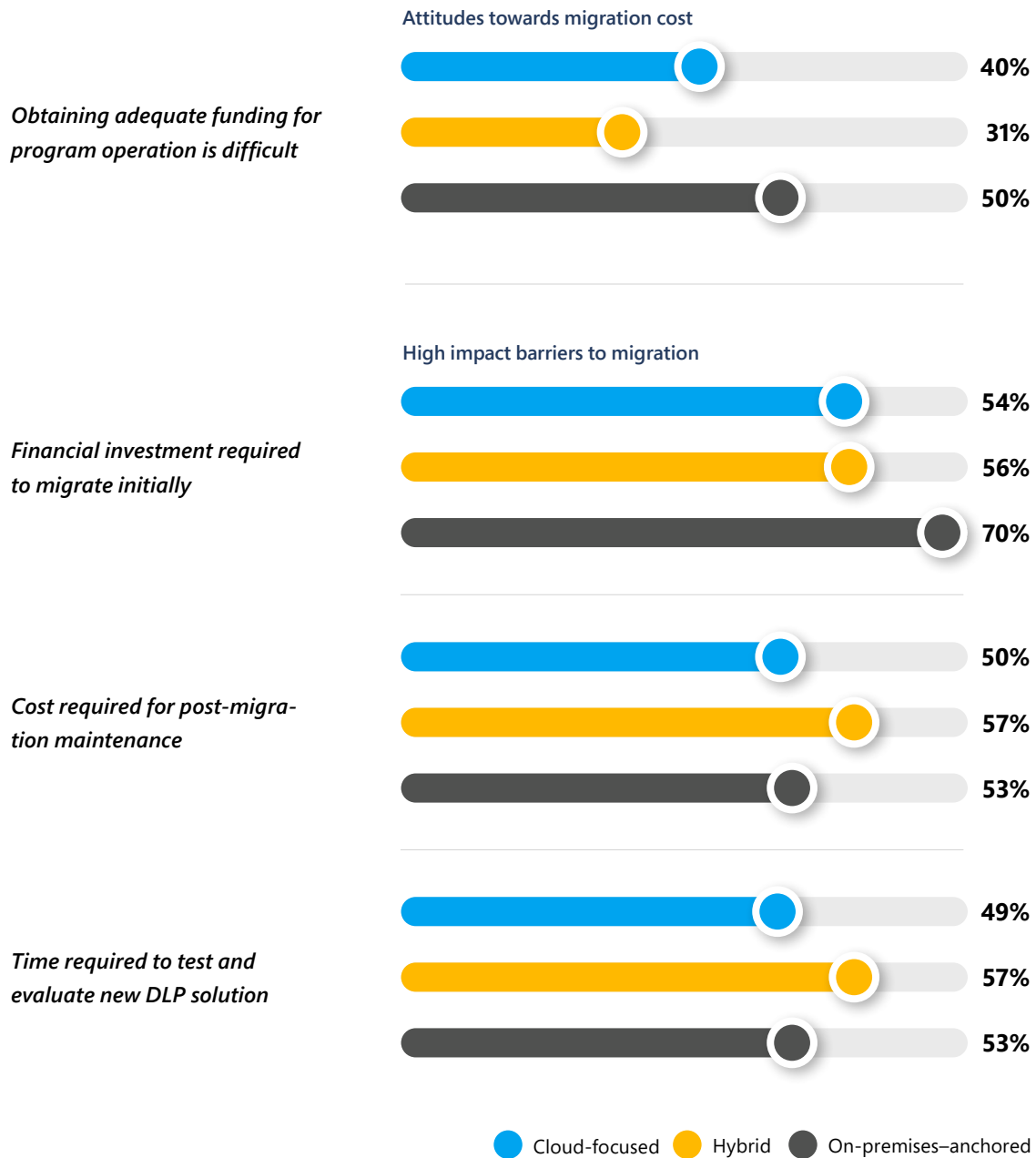
Organizations across all three states indicate to similar degrees that post-migration maintenance costs and the time needed to evaluate a solution are barriers to their firms further migrating to a cloud DLP solution.

*"The reason to migrate to the cloud is scalability. Whereas on-premises, it's a lot of additional cost to maintain physical servers, and they've only gone up."*

*CISO, Healthcare*

It makes sense that cost is a consideration for all. However, the upfront cost might be mitigated if it means that maintenance costs are less of a concern and fewer dedicated IT professionals are required—ultimately resulting in cost savings. Likewise, the initial investment of time and resources to make the move frees up time and resources to be leveraged elsewhere, benefits that hybrid and cloud-focused firms have already started to realize.

*"The overage charge you will get from utilizing cloud resources is less than the cost of us hosting in our own data center."*
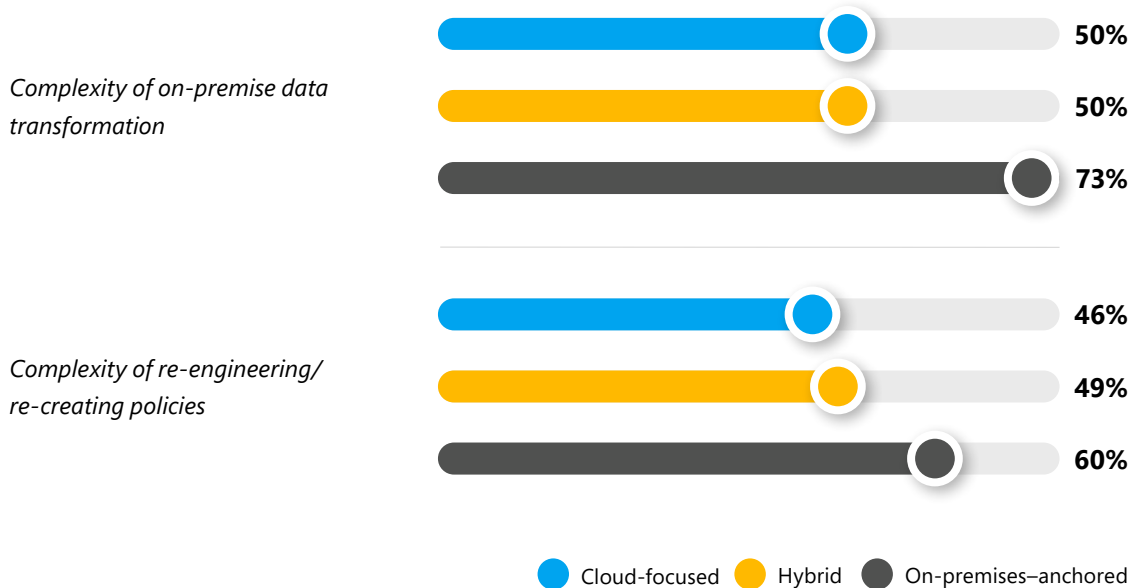
*CISO, Healthcare*

**Perceived complexity**

What happens once you start the migration process? What if you run into unexpected outcomes? The uncertainty surrounding the unknowns is driven by the high level of perceived complexity about the migration process. We observed anxiety associated with on-premises–anchored organizations around data transformation with 73 percent pointing to it as a top barrier *(figure 08)*. Likewise, we see half of hybrid and cloud-focused companies who've gone through at least some of the migration process, also stressing the high impact of data transformation to the overall migration experience.

Another top-level concern is re-engineering and recreating policies, with nearly 50 percent of all organizations reporting it's a challenge preventing them from taking the next step *(figure 08)*. The perceived complexity associated with migration drives anxiety and deters organizations from moving forward.

Figure 08: High agreement on the complexity of the migration journey

*Complexity of on-premise data transformation*

50%
50%
73%

*Complexity of re-engineering/ re-creating policies*

46%
49%
60%

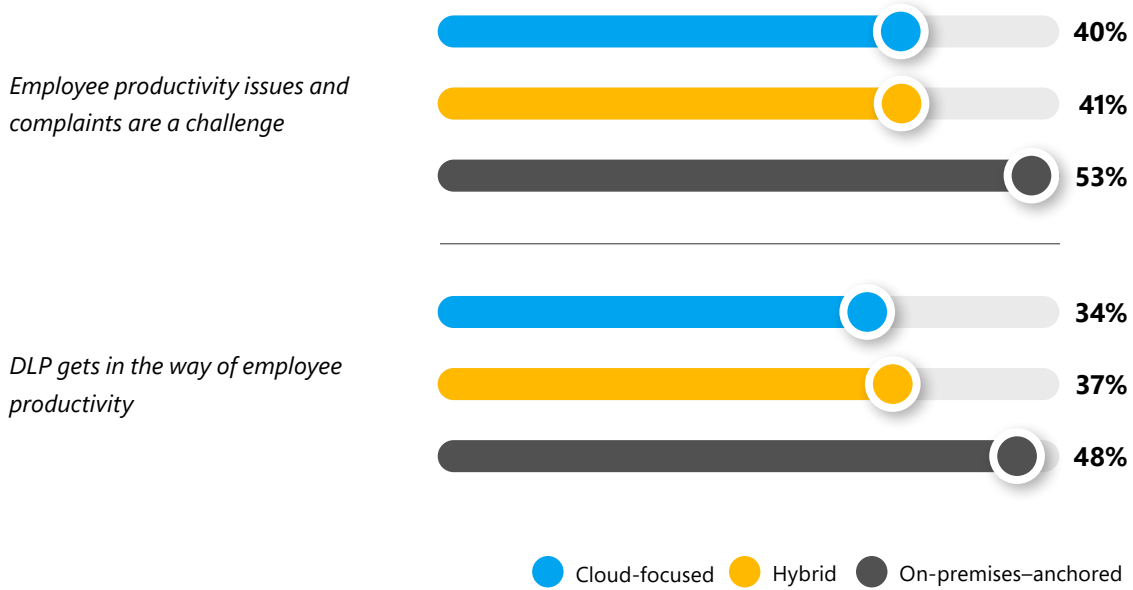● Cloud-focused   ● Hybrid   ● On-premises–anchored

*"I think the biggest issue right now is just getting our systems built and designed so they can operate up in the cloud. Because many of these systems are old legacy environments and they weren't designed for the cloud."*

**CIO, Healthcare**

## Productivity

Concern about productivity is another key area of differentiation. On-premises–anchored firms view impact on productivity as a much greater challenge; nearly half (48 percent in *figure 09*) say DLP gets in the way of productivity, whereas cloud-focused companies demonstrate the least concern around productivity impacts from DLP.

**Figure 09: Agreement of the challenge of productivity and DLP**

*Employee productivity issues and complaints are a challenge*

- 40%
- 41%
- 53%

*DLP gets in the way of employee productivity*

- 34%
- 37%
- 48%

● Cloud-focused   ● Hybrid   ● On-premises–anchored

*"We were concerned about DLP disrupting the business process. It's the day-to-day workflow of our business because we don't know what we don't know."*

**Cybersecurity executive, Utility Service**
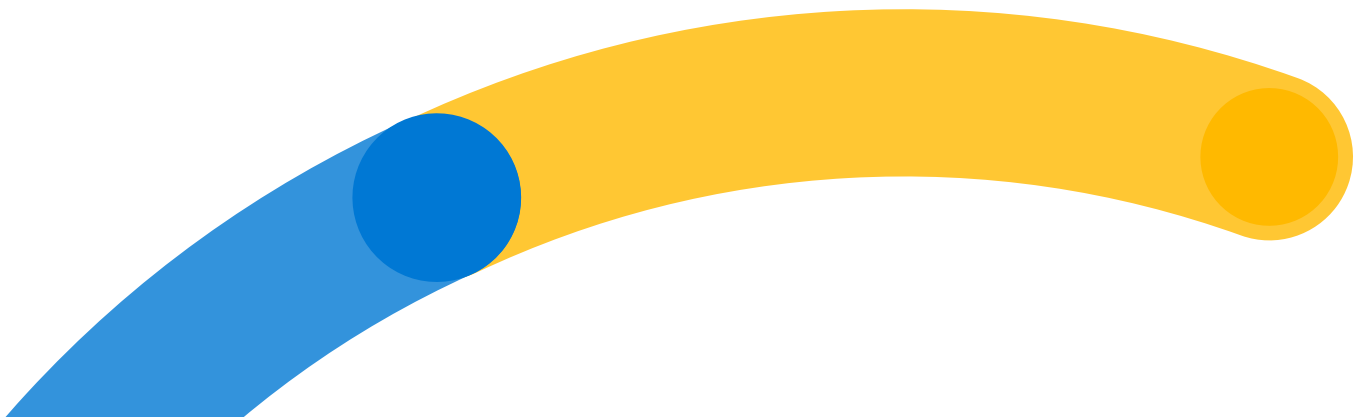
To further understand how companies were thinking about productivity, we looked at the mode in which their DLP solutions are running: audit-only or blocking.

In total survey results, we saw 50 percent of organizations were running DLP solutions in audit-only mode, while the other half were running in block mode. However, in *figure 10* on-premises–anchored organizations are more likely, at 58 percent, than hybrid or cloud-focused ones to run their DLP solutions in audit-only mode, reflecting a more reactive nature due to the perceived impact that blocking mode may have on productivity.

**Figure 10: Mode by DLP State**

| | |
|---|---|
| Block with override | 23% / 23% / 25% |
| Block Actions | 30% / 27% / 18% |
| Audit Only | 47% / 51% / 58% |

Cloud-focused  Hybrid  On-premises–anchored
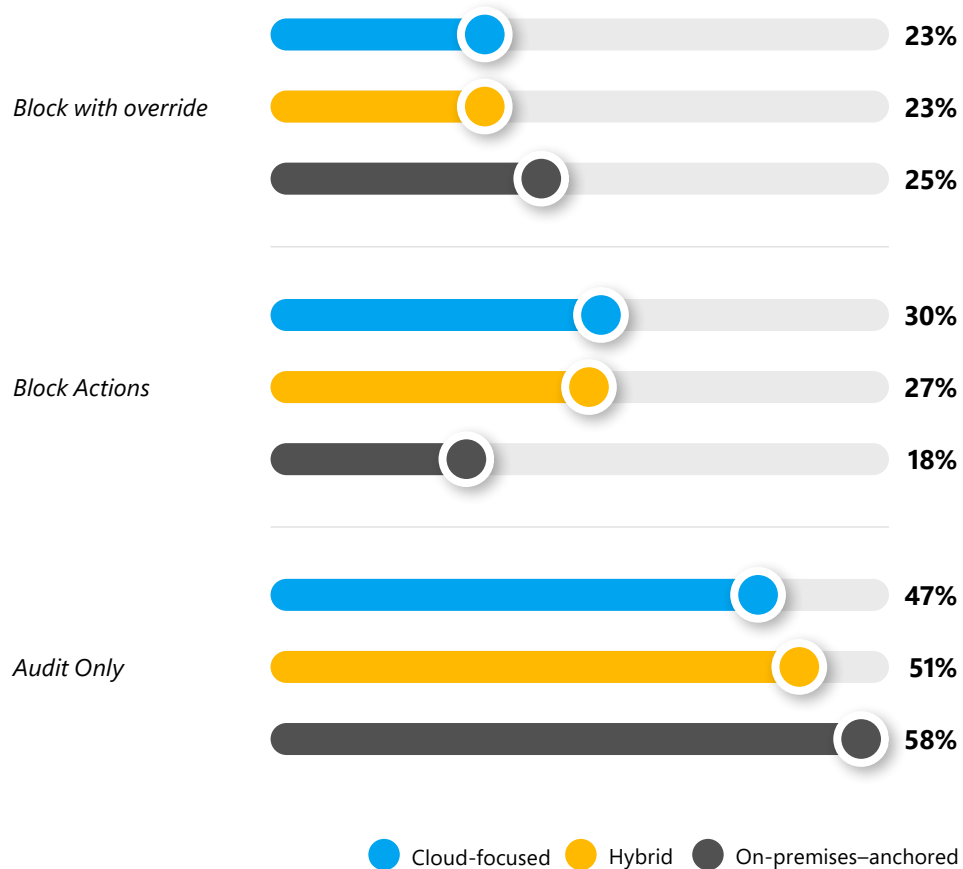
*"We are typically more reactive just by nature of the game."*

**Sr. IT Manager, Telecommunicationsm**

The balance between security and productivity is hard to strike for most organizations. While audit-only mode ensures there is no impact on productivity, it leaves the door open for data exfiltration—putting organizations in a reactive position with sensitive data at higher risk.

On the other hand, block mode is more proactive in nature providing a higher level of security and stopping events before they happen. This mode could be perceived by some organizations as impeding productivity, particularly among on-premises firms. However, by implementing more granular controls and better understanding around what type of data needs the most protection, organizations can strike the right balance.

For instance, an organization might decide that data from the Finance department is more sensitive and riskier than data from the Marketing department. This information can be used to set stricter policy controls for the Finance department to prevent data exfiltration from taking place by blocking inappropriate activity.

Cloud-focused firms have better control over DLP solutions that protect environments where data exfiltration is likely to take place, such as cloud productivity suites. This makes it easier for them to manage and set granular controls as well as enable educational tips to help employees enforce policies.

Meanwhile, on-premises–anchored firms are more likely to use the audit mode in part due to the higher level of apprehension about impacting business operations, productivity, and burdening IT staff. With proper controls as well as better employee education on data security risks, cloud-focused companies avoid this constraint.

*"It doesn't need to go to somebody's personal e-mail address or flash drive. It needs to stay in our environment. Our DLP solutions prevent sensitive data from being written or e-mailed or moved in any way outside of our organization."*
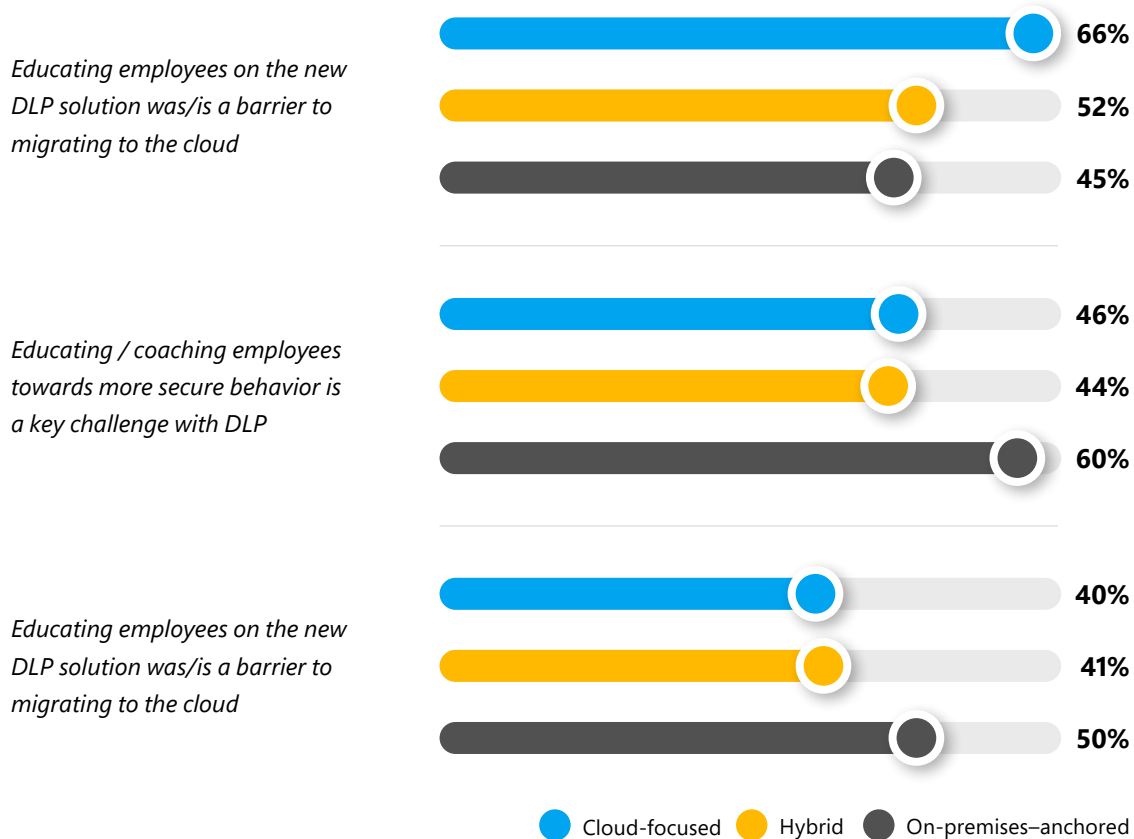
*CISO, Financial Services*

## Education

toward safer behaviors emerges as a challenge and a priority. In *figure 11*, 66 percent of cloud-focused organizations highly agreed employee education was a key barrier to migrating their DLP solution. Meanwhile, on-premises–anchored firms see education as a lower potential barrier to migration (45 percent). This suggests organizations that have gone through the migration process understand the challenges and expectations, while companies with less migration experience place a lower level of importance in this area because they haven't made the leap yet. This is a misplaced priority that on-premises–anchored companies should look to improve. From a holistic perspective, DLP education should reach the users to also include the policy makers.

*Figure 11* shows on-premises–anchored companies face a **higher** level of challenge educating employees on optimal data handling practices than the other states. The same is true for educating administrators toward better policy design. On the other hand, cloud-focused and hybrid groups reported a lower level of challenge around education, indicating they understand the importance of education as part of a holistic data protection strategy and have already begun addressing these problems. By prioritizing user education, organizations can decrease data exfiltration risk level and free up the administrators to focus on other high-priority issues—as there might be fewer alerts to triage and address.

**Figure 11: Education – Barriers and challenges**



Educating employees on the new DLP solution was/is a barrier to migrating to the cloud
- 66%
- 52%
- 45%

Educating / coaching employees towards more secure behavior is a key challenge with DLP
- 46%
- 44%
- 60%

Educating employees on the new DLP solution was/is a barrier to migrating to the cloud
- 40%
- 41%
- 50%

Cloud-focused   Hybrid   On-premises–anchored

"My biggest fear is that my own internal staff is my biggest risk. How do I train and better manage my staff to understand the risk that they put themselves and the company into?"

*CIO, Healthcare*

# What challenges do firms in regulated industries face?

Respondents in regulated industries such as financial services and healthcare are more likely to indicate greater challenges across several aspects of their DLP programs when compared to non-regulated industries. More than half (55 percent) of regulated industries indicate unstructured data is where they feel most vulnerable, higher than non-regulated. This aligns with the finding that regulated industries also place the highest priority on protecting data in collaboration applications.

Qualitatively, we heard legacy processes and prior investment in highly secure on-premises data storage often impede DLP efforts in regulated industries. This is in-part due to the higher level of regulatory requirements these organizations face, which dictates a traditional desire for more control over the data in order to comply with those regulations.

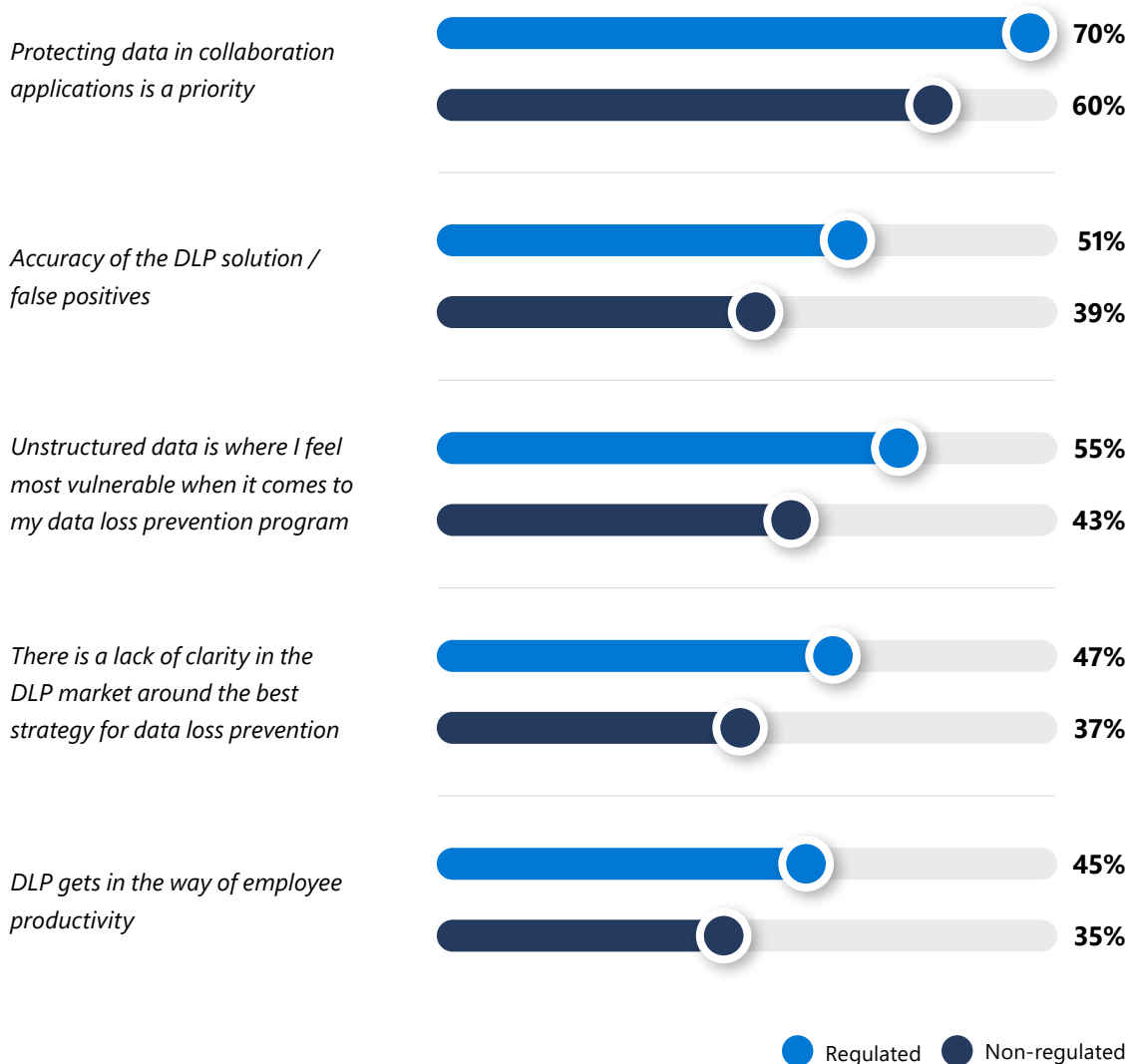*"A lot of business processes that organizations have rely on the transition of data that may not be secure because traditional third-party business partners that healthcare organizations have had don't pass secure processes."*

*CISO, Healthcare*

In *figure 12,* we see challenges with DLP alert accuracy (51 percent) and agreement that DLP impedes productivity (45 percent) are others area of differentiation between the two types of organizations. Indicating regulated companies are more likely to struggle with creating DLP polices that stop events from happening without flagging everything in sight. These differences along with their reported need for more clarity (47 percent versus 37 percent) align them closer to the companies that fall into the on-premises–anchored state and points to a need for evolving their DLP programs further on the continuum.

**Figure 12: Regulated/Non-regulated differences**

| | Regulated | Non-regulated |
|---|---|---|
| *Protecting data in collaboration applications is a priority* | 70% | 60% |
| *Accuracy of the DLP solution / false positives* | 51% | 39% |
| *Unstructured data is where I feel most vulnerable when it comes to my data loss prevention program* | 55% | 43% |
| *There is a lack of clarity in the DLP market around the best strategy for data loss prevention* | 47% | 37% |
| *DLP gets in the way of employee productivity* | 45% | 35% |

Regulated    Non-regulated

## A final note about uncertainty

We introduced this section with the notion of apprehension about the unknown as a challenge. On the positive side, respondents with greater experience migrating to the cloud indicate the journey is not as difficult as it seems: cloud-focused organizations were 46 percent less likely to say it's risky to switch solutions and 60 percent less likely to worry about losing control of their DLP program after migrating to a new solution. With the benefit of experience, cloud-focused firms are 35 percent less likely than the on-premises–anchored to say recreating policies from legacy DLP solutions is a major concern. Having been through a migration already helps minimize the discomfort around future uncertainty. They're closer to their ideal state and know what it takes to migrate—turning a previously unknown quantity into an experience to learn from for the next migration.

*"We had to do a lot of educational work, policy and procedure work, and technical work to ensure that people aren't sending data off. That's where DLP helps, because you've got to make sure people are sending data to the right place."*

*CISO, Healthcare*

# 05 DLP solution providers

To solve this long list of challenges and barriers, companies look for support from DLP providers. Interestingly, the organizations in earlier states on the DLP continuum evaluate DLP solutions significantly more often.

In *figure 13* we see on-premises–anchored companies are most likely to continually look for new solutions (35 percent) as they try to find a partner to help them, while hybrid organizations tend to evaluate solutions on an annual basis (44 percent).

The confidence expressed by the cloud-focused firms is displayed in their evaluation frequency at every 2 to 3 years (43 percent), showing they have found the partner solution that has helped ease their apprehension and reduce their challenge. Cloud-focused firms seem to evaluate every few years primarily to see if new features and capabilities may have been developed to help further their evolution.

**Figure 13: Frequency of evaluating DLP solutions**
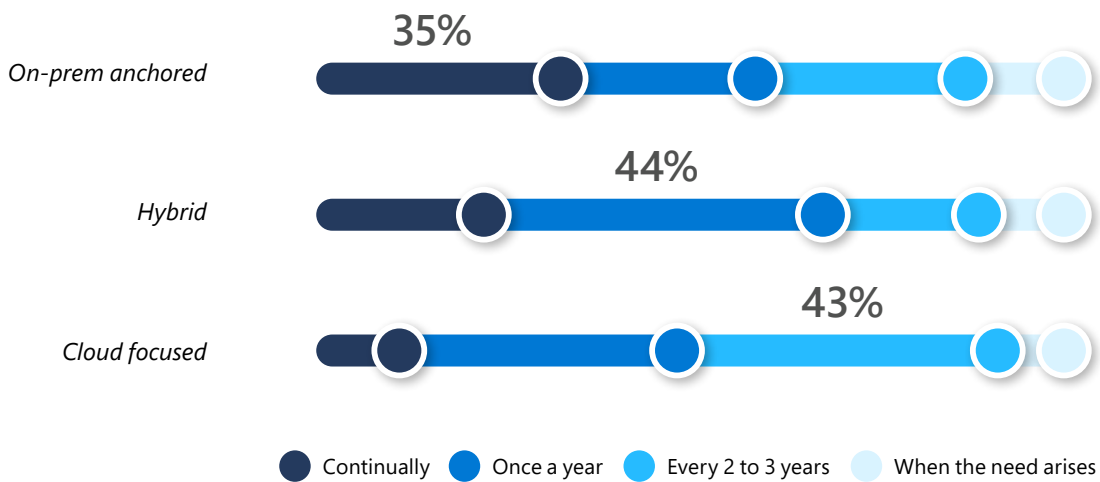


*"Every three years, we do a full evaluation. We'll see what's available [in the marketplace]. We won't necessarily switch, but we at least do that so that we can see if there were any major changes in the marketplace that might make us want to switch to a new provider."*

**CISO, Financial Services**

# Number of solutions

The size and variety of the data organizations are dealing with poses a complex environment for IT professionals, often requiring more than just one DLP solution.

On average, hybrid organizations are using about 20 percent more solutions than cloud-focused and about 15 percent more than on-premises–anchored organizations (see *figure 14*).

Our findings reveal on-premises–anchored organizations struggle to find the right solution to use, while hybrid firms continue to collect solutions to help them push forward. Hybrid organizations also have to put the time and effort into stitching together and maintaining their quilted DLP solutions—ensuring the solutions stay in sync and don't operate in silos. This is why building custom integrations is a high challenge for hybrid companies with nearly 50 percent indicating this. Meanwhile, cloud-focused companies have found what they need and are starting to consolidate.

*"It doesn't make sense to maintain two or three different solutions because then you have to keep them updated, you have to make sure that there's not a whole lot of difference between one, two, and three. So, you want to create the benefits and the economic savings of standardization. That's why consolidation is critical."*

**Director, Technology Services**

**Figure 14: Average no. of DLP solutions**

2.5

3.1
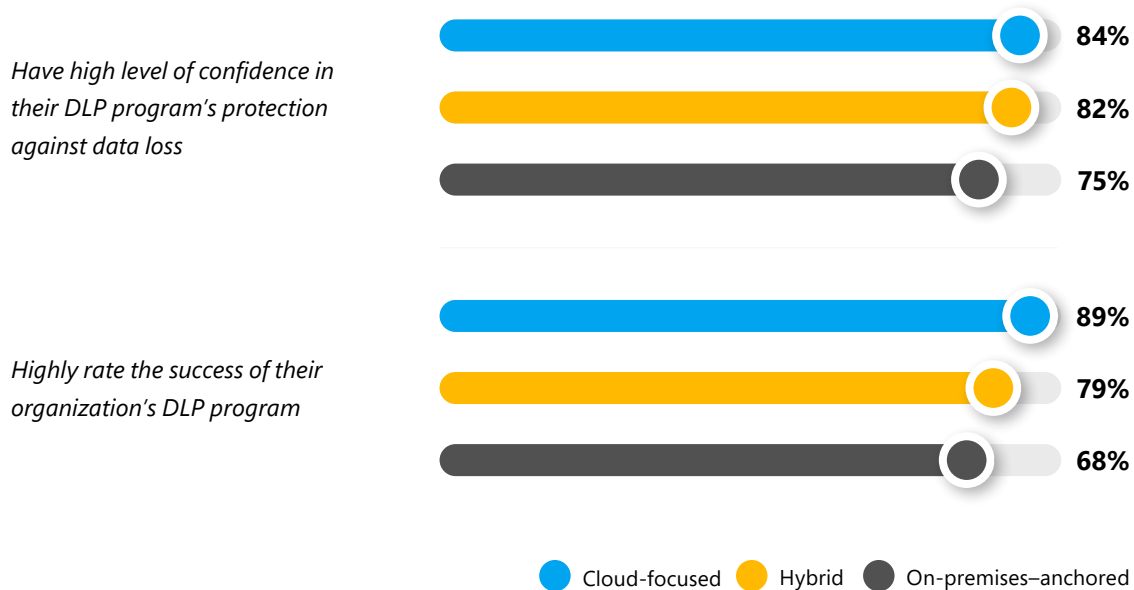
2.7

● Cloud-focused   ● Hybrid   ● On-premises–anchored
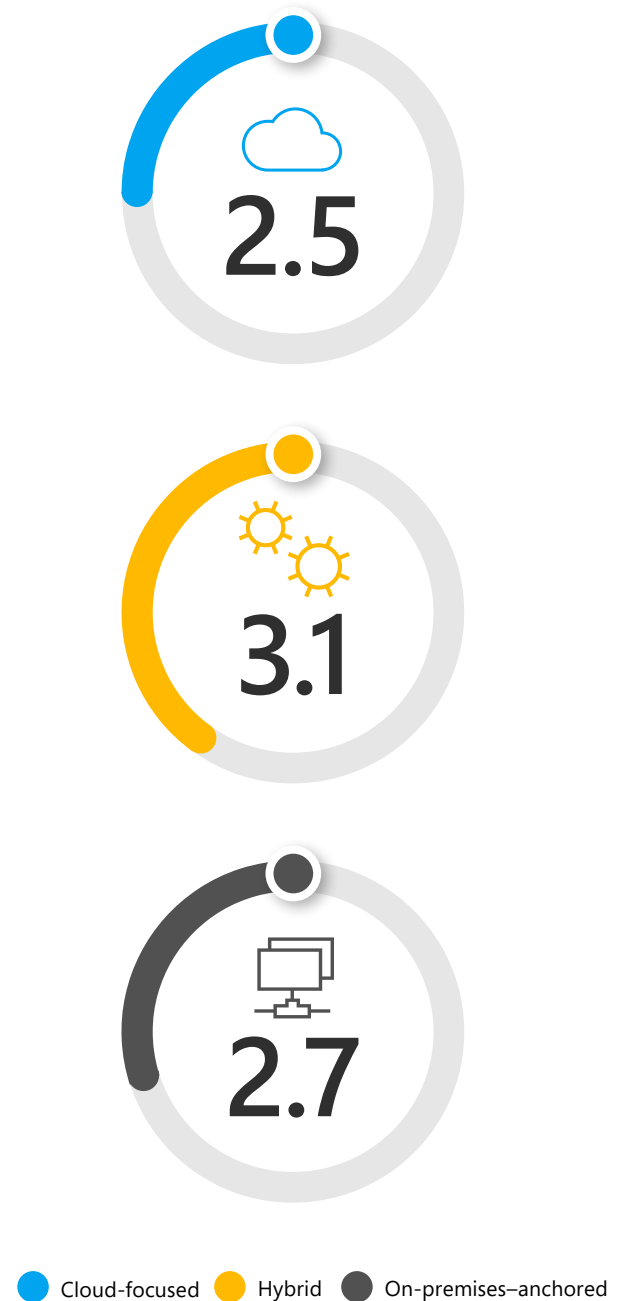
# 06 What does it all mean?

Most of our respondents possess some level of apprehension about the unknown, complexity, impacts to productivity, and cost. Yet most share the desire to move toward the cloud. Even the cloud-focused respondents expressed some level of discomfort about the unknown. However, it is outweighed by the true benefit of success and confidence they have experienced.

Confidence in their DLP program and perceived program success are higher with cloud-focused companies. Nearly 90 percent of cloud-focused respondents felt their program was highly successful (figure 15), while just 68 percent of on-premises–anchored felt the same way and 79 percent among hybrid. Despite this high level of perceived success cloud-focused companies still look to refine and improve their DLP approach, moving towards a cloud only state.

**Figure 15: Confidence and Success by DLP state**

*Have high level of confidence in their DLP program's protection against data loss*

84%
82%
75%

*Highly rate the success of their organization's DLP program*

89%
79%
68%

● Cloud-focused   ● Hybrid   ● On-premises–anchored

*"Data is just in all these places that you don't have direct control over and that can quickly become the Wild West. It's just a free-for-all that becomes really difficult to corral—kind of [like] a horse out of the barn."*

*Sr. IT Manager, Financial Services*

We know migration is expensive. We know budgets are tight. The pain of migration is real but history shows the inevitable progression of companies through the different states of DLP programs. Cloud-focused organizations face the uncertainty to get to this state and now report a lower level of challenge with their current DLP program because they've been through the process—compared to on-premises–anchored who report greater challenges.

We learned organizations in on-premises–anchored states are experiencing the most discomfort. They are in a perpetual state of considering and evaluating new tools and migration strategies. Meanwhile, hybrid respondents indicate they are comfortable where they are by reporting low current challenges and high confidence and success but are really just in a holding pattern—forced to spend time and effort on complex integrations and maintaining multiple DLP solutions in different data environments. As hybrid companies continue to evaluate what new DLP solutions are available, it's no wonder nearly all indicate they are exploring moving their current DLP solutions to the cloud to try and consolidate.

We also learned that while many respondents state they understand cloud DLP, there's an underlying complexity that drives a need for clarity. This opens up the possibility that some respondents might not in fact understand the pros and cons and be using the ideal approach to DLP.

*"Do we take this opportunity to change course and modernize the environment and give our end users more tools that allow them to be more productive? Especially in an age where people are still working hybrid most of the time?"*
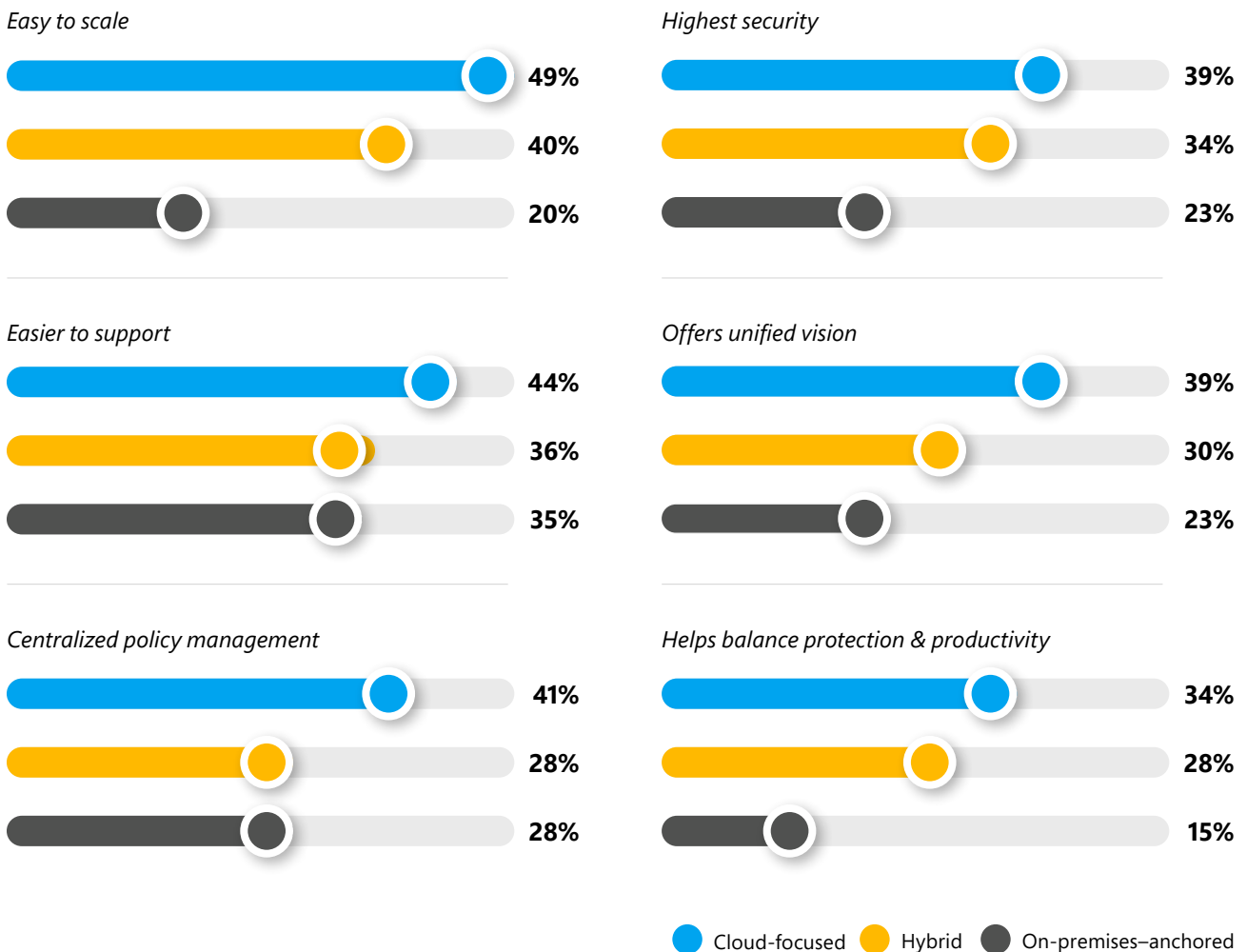
**Sr. IT Manager, Financial Services**
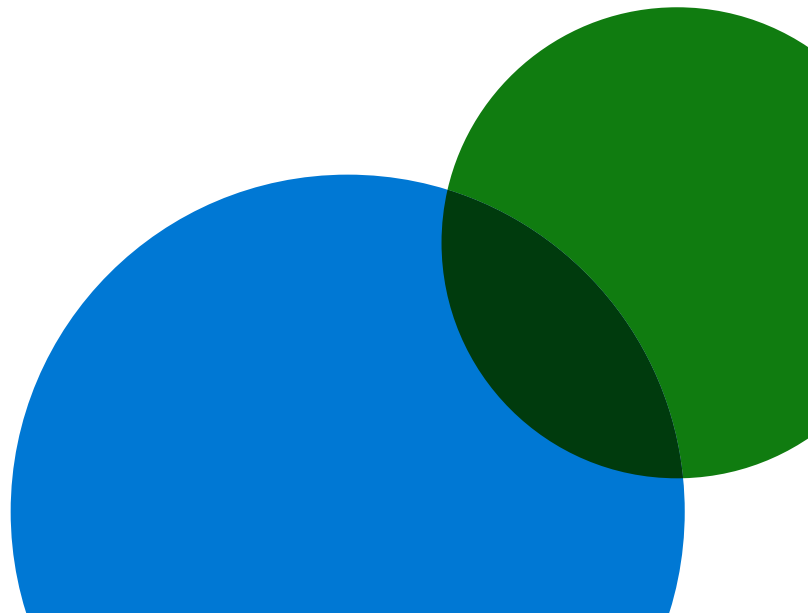
# Familiarity bias might cause hesitation

DLP professionals from cloud-focused firms were significantly more likely than those who are on-premises–anchored to indicate that cloud DLP offers significant benefits as compared to on-premises solutions—suggesting familiarity bias, a phenomenon in which people tend to prefer familiar options over unfamiliar ones, even when the unfamiliar ones might be better. Cloud-focused users recognize a superior experience once they have migrated to the cloud.

In *figure 16*, respondents in the cloud-focused DLP state feel it's easier to scale (49 percent), easier to support (44 percent), and offers better centralized policy management (41 percent). Both hybrid and on-premises–anchored respondents report less optimal results in the same categories.

**Figure 16: Strongly agree that cloud DLP offers this benefit**

*Easy to scale*

| | |
|---|---|
| Cloud-focused | 49% |
| Hybrid | 40% |
| On-premises–anchored | 20% |

*Highest security*

| | |
|---|---|
| Cloud-focused | 39% |
| Hybrid | 34% |
| On-premises–anchored | 23% |

*Easier to support*

| | |
|---|---|
| Cloud-focused | 44% |
| Hybrid | 36% |
| On-premises–anchored | 35% |

*Offers unified vision*

| | |
|---|---|
| Cloud-focused | 39% |
| Hybrid | 30% |
| On-premises–anchored | 23% |

*Centralized policy management*

| | |
|---|---|
| Cloud-focused | 41% |
| Hybrid | 28% |
| On-premises–anchored | 28% |

*Helps balance protection & productivity*

| | |
|---|---|
| Cloud-focused | 34% |
| Hybrid | 28% |
| On-premises–anchored | 15% |

Cloud-focused    Hybrid    On-premises–anchored

Moving toward the cloud and pushing through the uncertainty and anxiety of the challenges is critical for companies to evolve overall. The level of on-premises data a company holds is very much indicative of the DLP state in which they are likely to find themselves. The apprehension and cost of migrating their DLP solutions will go hand in hand with the ongoing difficulties of migrating their data and infrastructure. Finding slight advantages to deal with these large problems could be the difference between success and failure for some companies.

*"Cloud-native is a lot better because you're going to get the advantages of scale, and you're probably actually going to spend a lot less on your service costs because you're not running entire operating systems or computers, you're literally running services, and you get billed for the compute time on the services, not that compute time for having to run in a data center."*

*CISO, Healthcare*

## What are the differences between cloud-based and cloud-native DLP solutions?

**Cloud-based:**
Integrates with your existing cloud and on-premises environments but isn't natively built in the cloud environment and/or productivity suite. To work, it relies on installing and updating agents and custom integrations. Many cloud-based DLP solutions started out on-premises and evolved into the cloud.

**Cloud-native:**
Built into the cloud environment and productivity suite by the cloud and collaboration tools' provider. Cloud-native solutions are built in the cloud from the start and are thereby already in the state in which most programs are moving toward.

# Benefits of leveraging a cloud-native DLP solution

*"It's always better to get something that is native to the environment you're working in. It's also significantly more cost-effective to manage it that way."*

*CIO, Healthcare*

If your company already has data in the cloud—which we found most of the organizations on the DLP state continuum did—you have two options to protect your data: use a *cloud-based* or a *cloud-native* DLP solution. **Both** types of solutions will require recreation of policies. However, there are advantages in cost and simplicity associated with cloud-native solutions as they are already built into cloud environments.

While cloud-based solutions also work with cloud environments, they are not natively built into the cloud environment and require complex integration efforts to make the solution work. These integrations add extra hops to the protection process, which can impact latency and performance. Likewise, organizations can expect to have more maintenance and upgrade costs, as agents will be necessary to make the solution work on endpoint devices.

On the other hand, your cloud environment will likely have a cloud-native DLP solution built in already as part of the offering, which can eliminate the need to procure and implement a separate

cloud-based solution. Cloud-native DLP solutions can also alleviate some of the challenges and barriers associated with migration overall.

For instance, cloud-native DLP solutions don't require agents because capabilities sit within the service itself and therefore don't need to be present on endpoint devices—this makes it easy to deploy, maintain, and save costs in the short and long-term and eliminates the need to hire specialized talent to support the migration effort and ongoing maintenance after the fact. Likewise, since there is no hardware to oversee, all updates are automatically implemented without heavy IT department intervention—which is especially vital for those times when resourcing is an issue. Lastly, since everything is natively integrated, DLP controls are more streamlined resulting in better performance and lower latency, which positively impacts workforce productivity.

*"I see the cloud as an extension of our enterprise infrastructure. My viewpoint is get it into the cloud. They can do security, capacity, and availability better than me. If my data is moved up there, then my DLP solution needs to be in there as well."*

*CISO, Telecommunications*

# Best practices for migrating your DLP solution to the cloud

Ensure you and your organization aren't left behind. By confronting caution and apprehension, you too could achieve the ideal state of a robust DLP program that yields confidence and success.

## 1. Use a cloud-native DLP with a holistic approach

A cloud-native DLP solution will have capabilities already built-in to the services to help you identify and protect sensitive information across workloads and devices. However, don't stop there. Check to see if the partner you are evaluating offers integrations with other solutions that are key elements of a holistic data protection strategy, including the ability to classify and label data as well as address insider risks. Look for solutions that offer trial periods to see the benefits for yourself and alleviate uncertainty and anxiety that might be preventing your organization from taking the step forward.

## 2. Choose the right solution provider and take advantage of migration tools

We know that migrating policies from one DLP solution to another is complex and involves reengineering and recreating policies. Seek out a solution provider that understands the challenges— one that offers migration tools that automatically convert policies from legacy solutions to reduce the manual work and mitigate the pain and anxiety that might arise in the process. A provider who offers documentation and support adds value to firms with questions about migration or solution adoption.

## 3. Recognize your apprehension and overcome it

Migrating to a new DLP solution surfaces questions and unknowns that might generate apprehension. However, as organizations move more data into the cloud, they start to see the DLP ideal state. Data protection capabilities offered by cloud DLP solutions come with significant benefits that can help ease uncertainty and mitigate future pain points. While there are challenges and barriers associated with making the move, don't let them hold you back. Take the time to identify the challenges and barriers specific to your organization and weigh those against the beneficial outcomes of migration.

## 4. Ensure security without compromising productivity

Proactively protecting data by blocking DLP events before they happen is a better policy approach. But striking a balance between data protection and productivity remains a prominent area of focus for all companies. Organizations should block actions and find solutions that allow for a more granular level of policy making to provide administrators a greater level of control.

# Conclusion

Organizations need to evolve as the data landscape continuous to change. Relying on traditional methods keeps organizations static and impedes progress towards a cloud-focused DLP state. Sticking to traditional methods also prevents companies from actualizing tangible benefits, such as those associated with a cloud-native DLP solution.

When adopting a cloud-native DLP solution organization can save costs by eliminating the need for infrastructure deployment and maintenance as well as custom integrations—driving more consolidation by removing silos. Organizations can also see improved performance, which can help drive productivity, as there are less hops for the data to travel through since everything is built-into the cloud applications and services. For the same reason, scaling DLP policies to other workloads is easier and takes the burden off already constrained IT departments.

To effectively protect sensitive data, while balancing organizational productivity, companies should look to be more proactive in their DLP approach. Finding the right solutions, with supporting tools, will help ease the apprehension associated with migration and will help your company unlock the benefits of a cloud-native approach.

*"Moving to a cloud DLP solution demonstrates our core value of excellence by demonstrating that we are investing our time and resources to providing the best care for our patients, providing the best experience, and ensuring their safety and security not only through data but through all the processes that we follow."*

**CISO, Healthcare**

# 0A Appendix

## More about the study

Let's review our research methods and who we surveyed for this study.

**Research methods**

This study was commissioned by Microsoft and conducted by Concentrix Catalyst. We surveyed and interviewed a total of 307 United States-based DLP professionals and compliance decision makers from companies of a variety of sizes and industries to understand their current approach to DLP, perceptions of benefits and drawbacks of cloud solutions and barriers to cloud migration of DLP solutions.

Our fieldwork was conducted over a five-week period during November and December 2022. The researchers utilized quantitative surveys and qualitative interviews to capture and extrapolate data. Our final benchmark sample consisted of 297 separate respondents and an additional 10 qualitative interviews.

Organizations featured in this study included the following characteristics:

- 1000 or more employees

- In commercial or public sector

- Based in the United States

- Respondents include Senior Managers, Data Administrators, Directors, Senior Directors, Vice Presidents, and C-level information security professionals across functional areas like compliance/risk management, human resources, information technology, legal and operations/production involved with managing, implementing and/or selecting DLP solutions for their organization
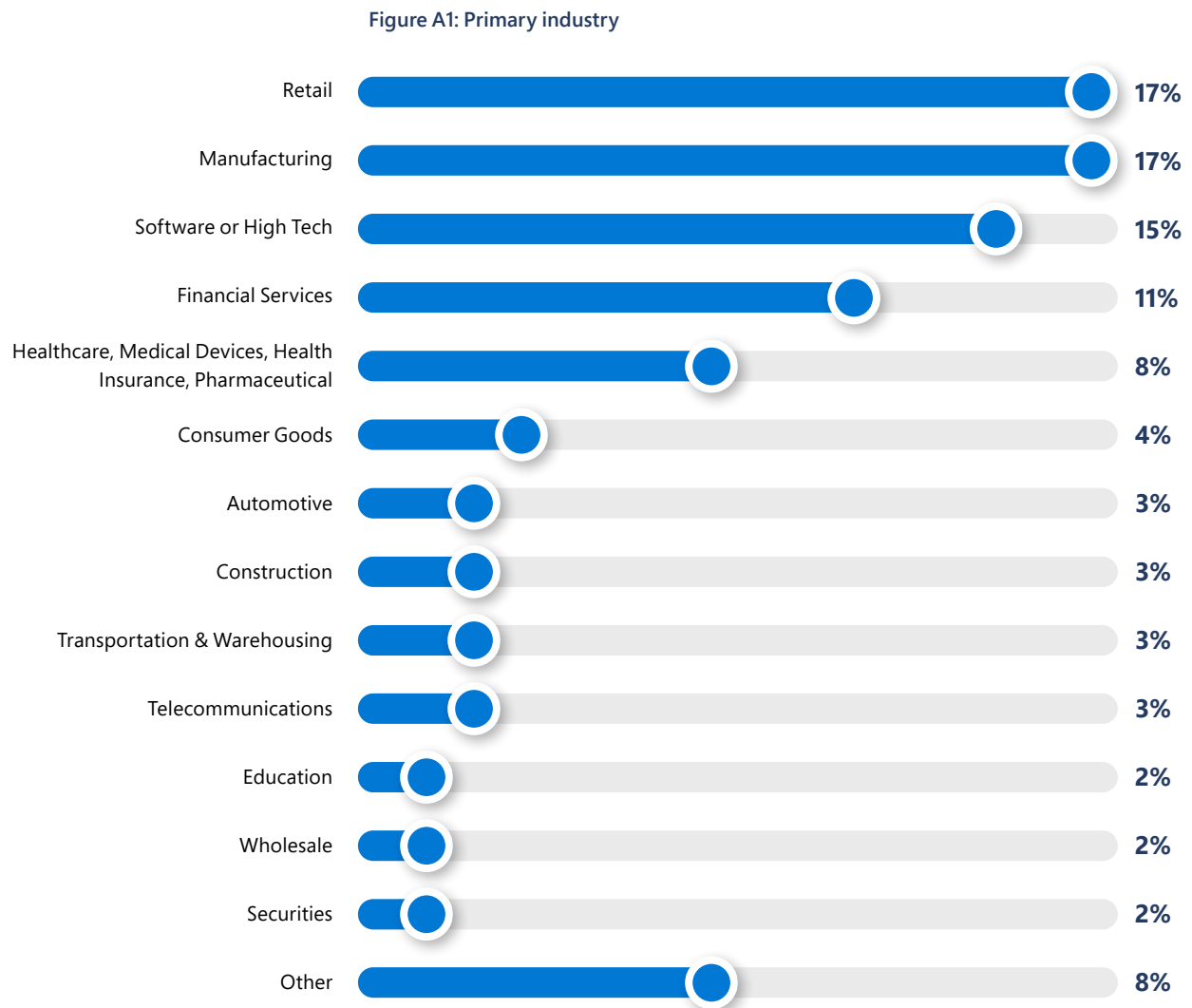
**Composition**

- 297 United States-based DLP professionals and compliance decision makers completed a 12-minute online survey

- 63 percent of survey respondents were categorized as "hybrid," 24 percent as "cloud-focused," and 14 percent as "on-premises–anchored"

# Who we surveyed

## Industry sectors

The four largest industry segments were retail, manufacturing, software or high tech, and financial services

**Figure A1: Primary industry**

| Industry | |
|---|---|
| Retail | 17% |
| Manufacturing | 17% |
| Software or High Tech | 15% |
| Financial Services | 11% |
| Healthcare, Medical Devices, Health Insurance, Pharmaceutical | 8% |
| Consumer Goods | 4% |
| Automotive | 3% |
| Construction | 3% |
| Transportation & Warehousing | 3% |
| Telecommunications | 3% |
| Education | 2% |
| Wholesale | 2% |
| Securities | 2% |
| Other | 8% |

## Company size

Nearly 6 in 10 respondents (59 percent) came from companies with between 1,000 and 5,000 employees.

Just over one-quarter of the respondents (26 percent) came from companies with 5,000 to 10,000 employees and the remaining 15 percent came from organizations with 10,000+ employees

- 1K-4.99K
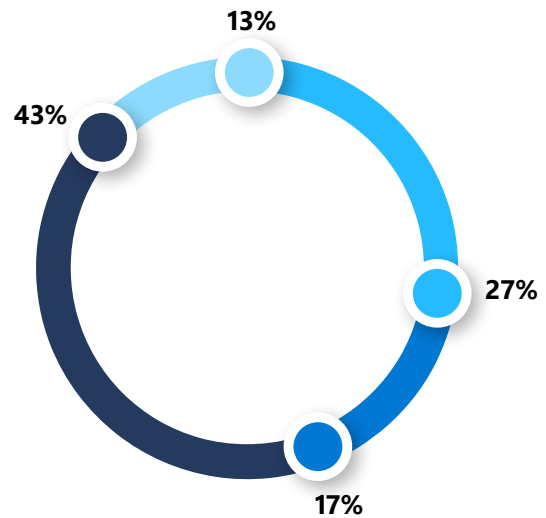- 5K-9.99K
- >10K

**Figure A2: Company size**

59%

15%

26%
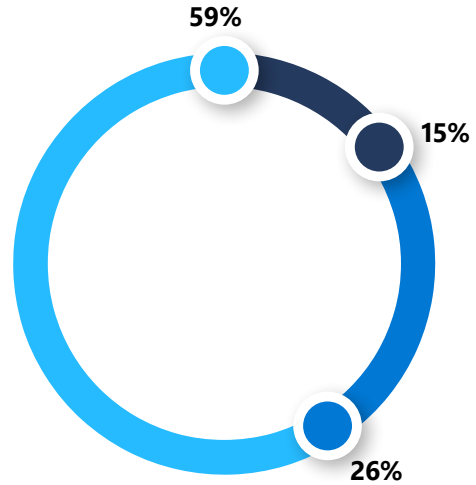
## Position level

More than one-quarter of respondents (27 percent) were at the VP/C-level; 60 percent were at the Director/Sr. Director level and 13 percent were at the Senior Manager level.

- C-level/VP
- Sr. Director
- Director
- Sr. Mgr/Admin

**Figure A3: Position level**

13%

43%

27%

17%

# References

[1] **Page 05**
"Guard Your Competitive Edge And Maintain Trust
With Data Privacy And Security,"
*Forrester Research, Inc. (January 25, 2022)*

[2] **Page 07**
"Building a Holistic Insider Risk Management
Program: 5 elements that help companies have
stronger data protection and security while
protecting user trust,"
*Microsoft Security white paper, 2022.*

[3] **Page 13**
"Guard Your Competitive Edge And Maintain Trust
With Data Privacy And Security,"
*Forrester Research, Inc. (January 25, 2022)*

[4] **Page 13**
"Building a Holistic Insider Risk Management
Program: 5 elements that help companies have
stronger data protection and security while
protecting user trust,"
*Microsoft Security white paper, 2022.*

[5] **Page 15**
"The State Of Privacy, 2022,"
*Forrester Research, Inc. (September 22, 2022)*