INDUSTRY REPORT

Data@Risk

A Global Industry Analysis

zscaler™

Table of Contents

Your Data is at Risk. Who's to Blame?

Enterprise data is now more vulnerable and difficult to protect than ever before. However, the main cause may surprise you. It isn't simply that threat actors are becoming more prevalent and sophisticated (although they are), it's that users are more distributed than ever and are becoming increasingly comfortable working outside the office. With hybrid work becoming the new normal and convenience taking precedence for most users, security can sometimes be an afterthought—until it's too late.

Ultimately, this hybrid work paradigm shift requires IT leaders to challenge their security assumptions and adapt to their new reality. This report details the findings of **Zscaler's 2021 Data@Risk Global Industry Survey, conducted in partnership with Cite Research**, which proves that organizations worldwide still have much to do in order to secure an increasingly remote workforce.

A Remote Work Pulse Check

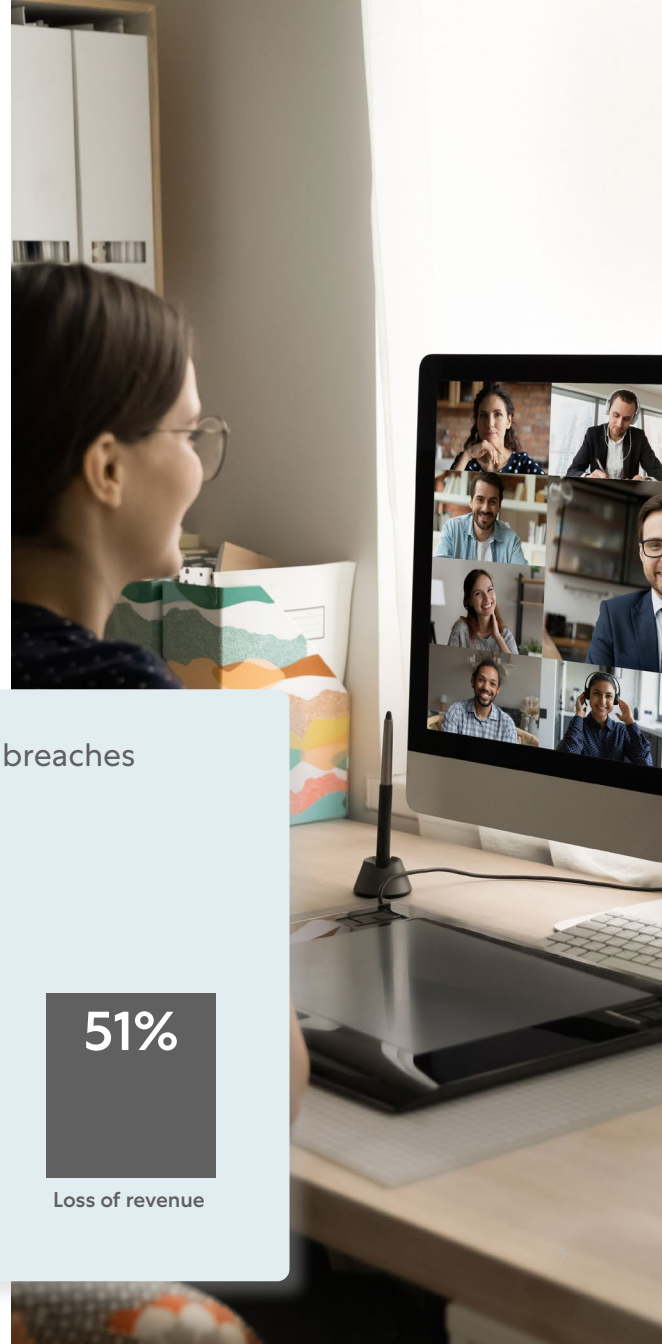
The global pandemic has turned the workforce model inside out. Gone are the days when innovation only happened within the walls of the corporate office. With this shift comes a host of new challenges. Are organizations and their IT departments optimized for the new frontier of hybrid work?

Remote work needs some work

Remote work has undoubtedly changed the game, and it's clear that it is here to stay. Organizations need to offer remote work to stay competitive, and employees often claim to be more successful and productive in a remote work environment.

In our analysis, we asked **500+ IT professionals** if they saw an increase in remote work **over the last 12 months**. Unsurprisingly, almost all of them said yes.

But here's the twist: we asked those same respondents if data breaches increased since remote work began, and, if so, what the impact was of those breaches. Almost three quarters of respondents said breaches increased during remote work. Surprisingly, the largest impact of these breaches was a decrease in productivity, the very thing remote work seems to help increase.



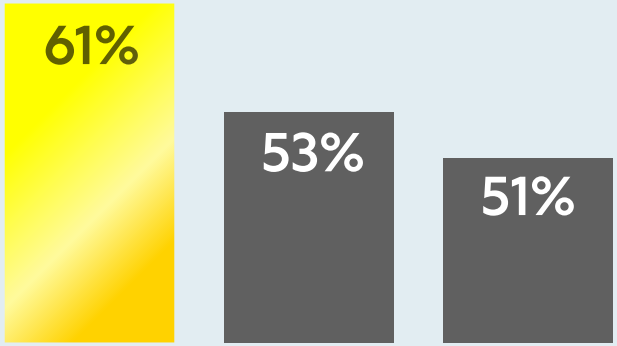
95%

Organizations that saw remote work increase due to COVID

75%

Organizations that saw data breaches increase since remote work began

Impact of those data breaches



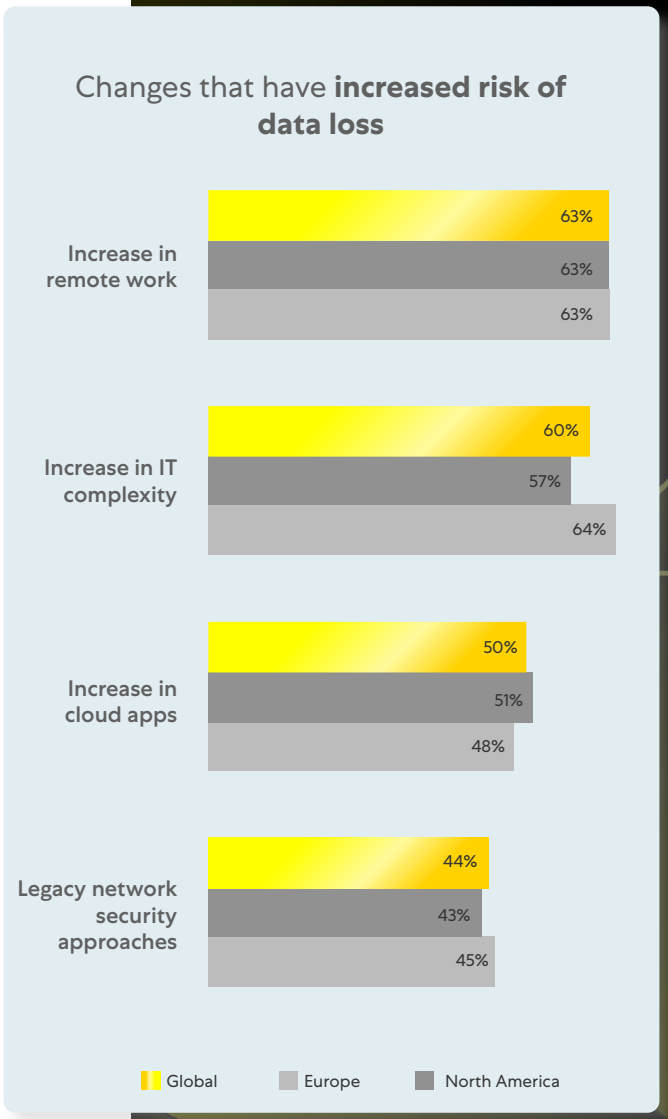
Is remote work really to blame?

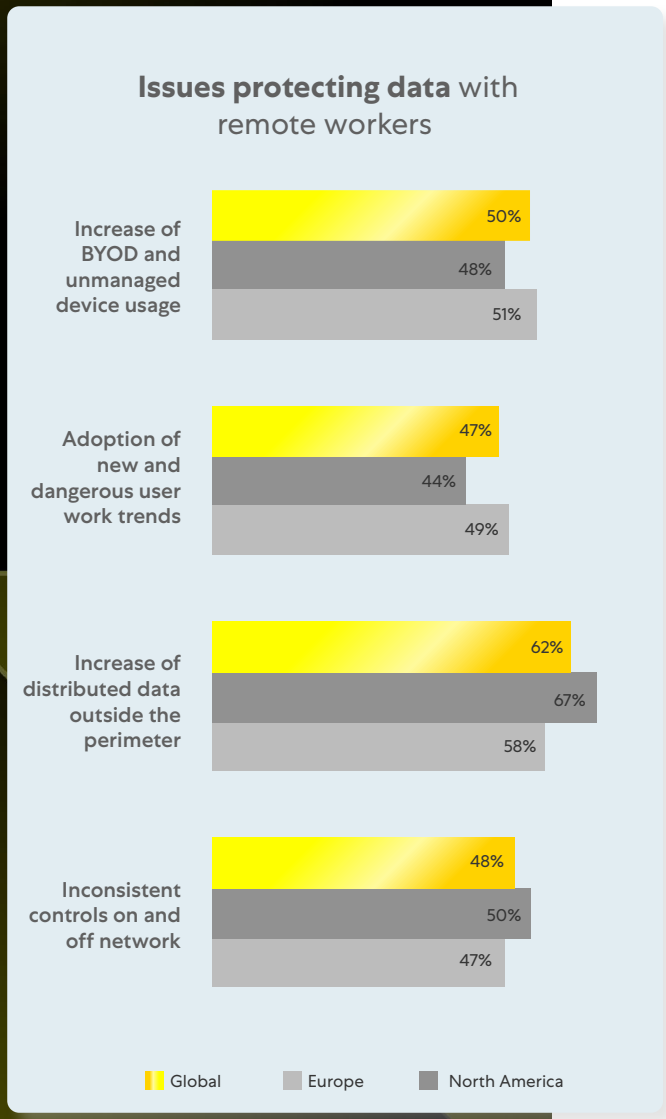
Let's zoom out to understand what factors are driving data risk across the organization. While we can see that remote work leads the pack, IT complexity and cloud applications carry a fair share of the blame.

TAKEAWAY

While remote work and cloud apps are great for business enablement and continuity, they also increase complexity across the IT landscape and aggressively distribute data outside the perimeter.

In the face of these changes, IT organizations often struggle with enforcing legacy security approaches, as highlighted in their responses.





Risks facing your data

How are these new challenges driving risk? The common theme is **loss of control** – which has always been a critical challenge for IT. Do you have control over users and data that can help pre-empt the risk of bad decisions?

TAKEAWAY

Remote work has empowered users to take productivity into their own hands by adopting new habits and devices (BYOD). Ultimately, the collateral damage of these dangerous trends is your data.

Additionally, data has left your data center (the control center), which leads to inconsistent security off network (when away from data center).

Preparing for Hybrid Work

As we enter the next step in the evolution of the modern workplace, what should IT organizations be thinking about to help embrace hybrid work while maintaining visibility and control?

Preparing users: where to focus

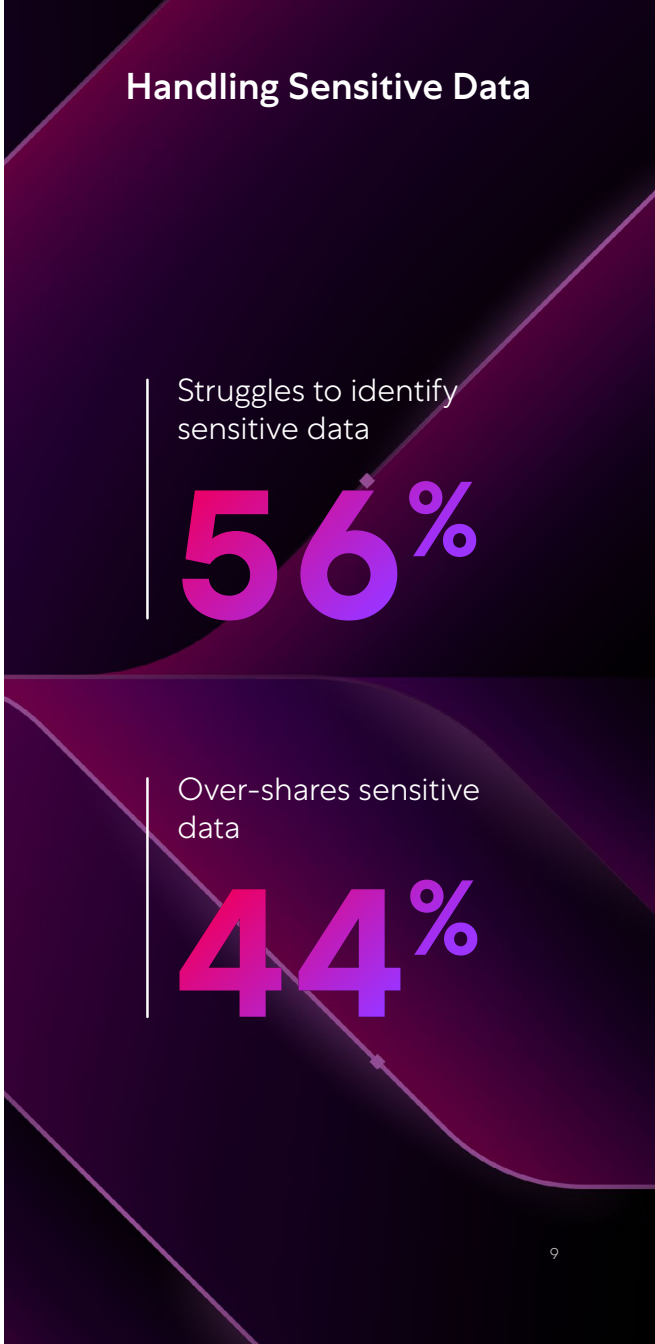
What users are **stuggling with due to remote work:**

Education on handling sensitive data

Of the 500+ respondents, more than 40 percent stated that users struggle to understand how to handle sensitive data. Of this group, more than half reported that users can't identify sensitive data, while the rest said users over-share this sensitive data in risky ways.

TAKEAWAY

IT leaders need to make sure data protection technologies don't operate in a vacuum. They should adopt aggressive programs to highlight violations so users understand their mistakes, as well as explore document tagging (like Microsoft AIP) to better control and highlight data.



Preparing users: where to focus *(continued)*

Circumventing corporate solutions

Using personal devices

35%

Using personal apps

34%

Bypassing security

31%

Enforcing the use of corporate solutions

The remainder of the respondents reported that users are adopting personal approaches to work instead of utilizing corporate solutions. Whether it's using personal devices and apps or bypassing security, users are clearly looking for more productive ways to get their work done and are unknowingly increasing risk.

TAKEAWAY

Remote work can isolate users and impact their understanding of how to use corporate solutions effectively. Organizations must improve IT communication around approved solutions and closely monitor shadow IT trends. They also should embrace a multimode CASB that can deliver both inline and API control over cloud app and security, without impacting user experience.

Preparing IT: where to focus

When we asked respondents about their biggest challenge for handling sensitive data, the answers were somewhat distributed, but still telling.

IT and user collaboration

About 27 percent of IT respondents are struggling with developing programs that help users identify sensitive data. At the same time, 13 percent are struggling to educate users on where data resides. With how dynamic and distributed your data is today, this challenge calls for a collaborative approach.

TAKEAWAY

Organizations should improve IT visibility, which can then be used to better prepare users. They must also embrace inline and API-based cloud DLP that spans all users and devices, in all locations. Regardless of whether policies are alerting or blocking, companies must find ways to alert users of their mistakes. Internal training can help highlight examples of sensitive data relevant to the company.

Preparing IT: where to focus *(continued)*

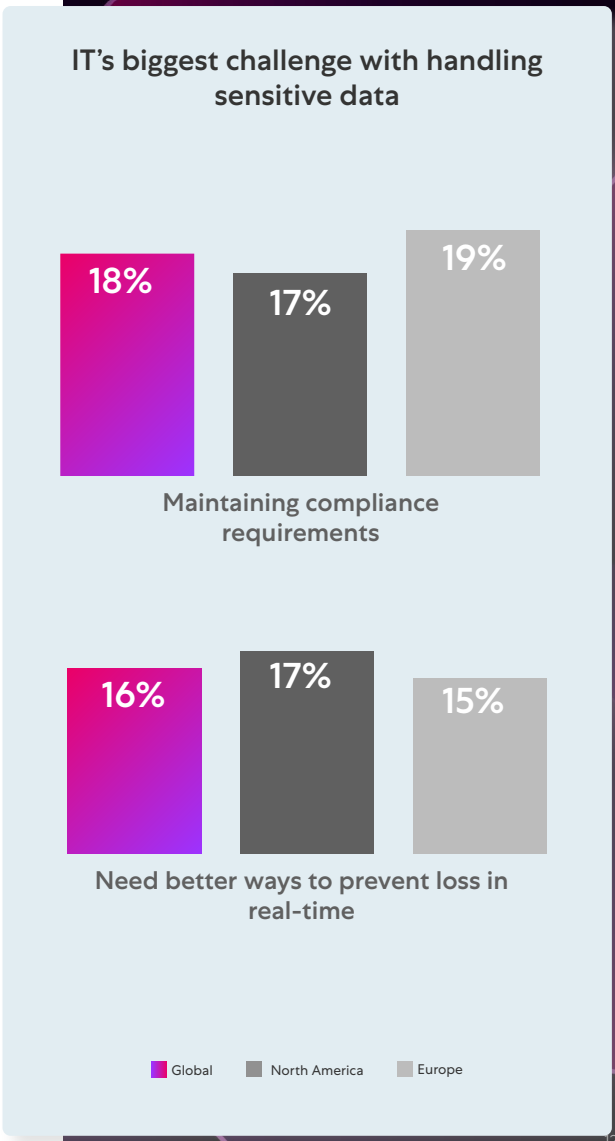
Other respondents described their greatest challenge with handling sensitive data differently.

Data protection hygiene

It's no surprise that the remaining 60 percent of the 500+ respondents are looking for better data control. From the lack of real-time blocking to difficult policy and compliance management, countless issues are often by-products of legacy IT debt. As today's norm has shifted to remote work and the cloud, legacy approaches have started to lose their effectiveness.

TAKEAWAY

Even in the short term, improved visibility can help guide IT into the right data protection decisions. Once the location and access patterns of sensitive data are understood, organizations can better enable decisions that ease the burden of enforcing policy, compliance, and inspection.

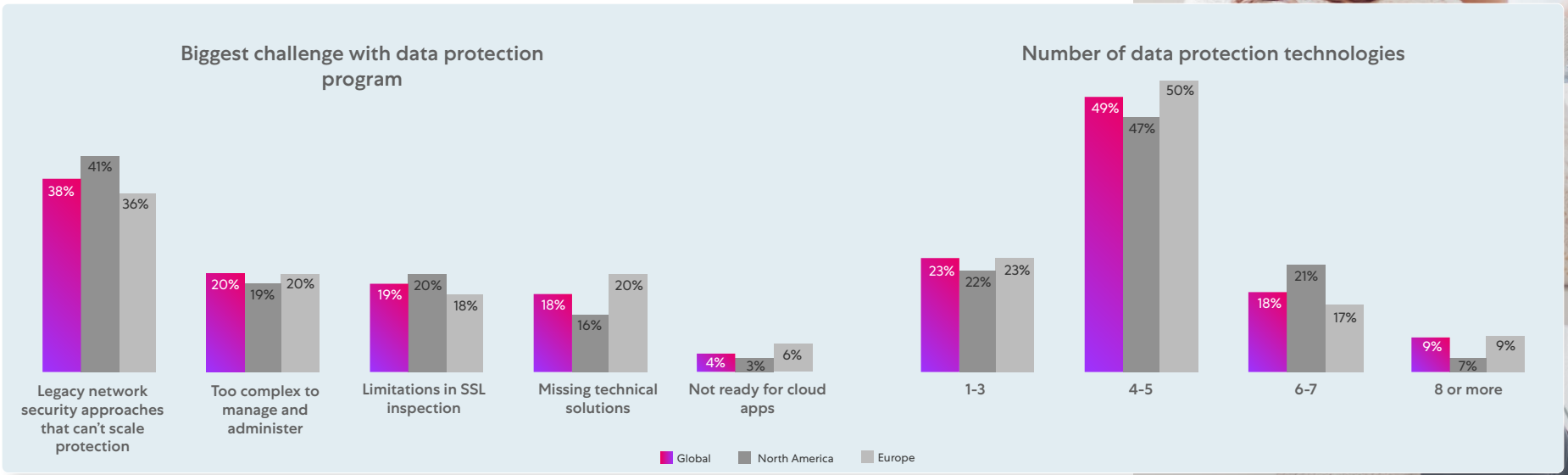


Preparing security: where to focus

Are today's organizations properly equipped to secure hybrid work? Almost **40 percent** claim that their current approach to network security **can't scale to their needs**. Other challenges are rooted in complexity, a lack of SSL inspection, and the absence of needed technical solutions. It's no wonder organizations are struggling, with more than **75 percent** of respondents managing **four or more data protection solutions**.

TAKEAWAY

By their nature, IT environments go through iterative changes that often cause security programs to take one step forward and two steps back. Avoid the "shiny new toy syndrome," and carefully map your three-year security strategy. Cloud apps and the hybrid workforce demand a new approach to security. Organizations need platforms that can reduce complexity, grow with enterprise needs, and secure all your cloud and mobile use cases.



Improving Data Defense

Where are organizations looking to invest in the future? With the many challenges that come with securing hybrid work, the results are telling.

Doubling Down on Distributed Data

When we asked our 500+ respondents to take stock of their data security, we first wanted to validate what they are trying to solve. With the rise of cloud apps and remote work, it's no surprise that data has left the building and is more at risk than ever.

Respondents who agree that more sensitive data is located outside the parimeter than in the data center:

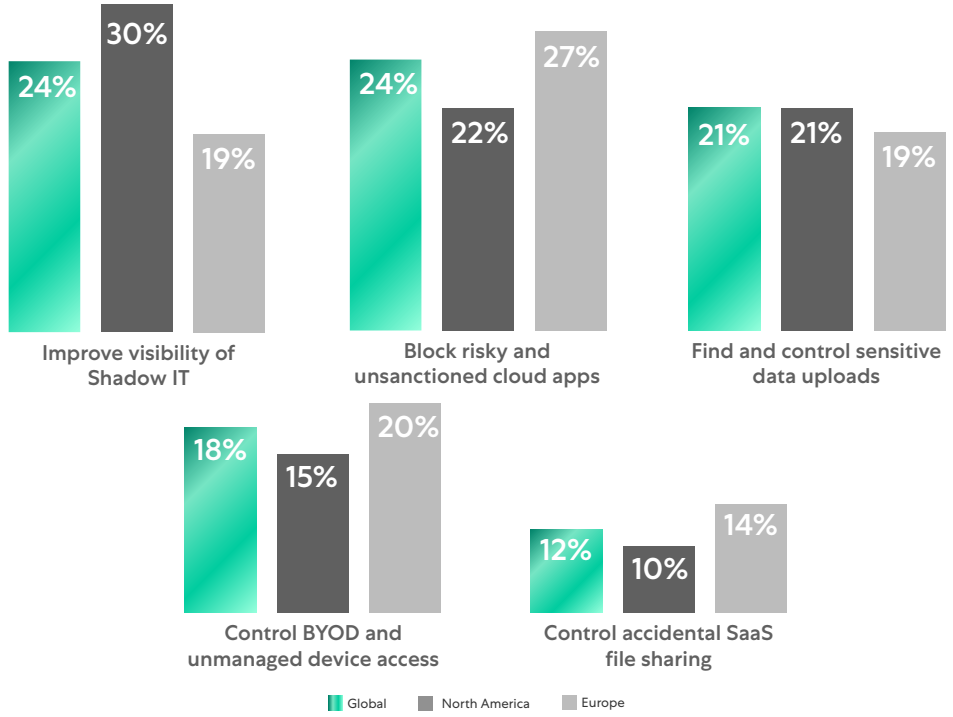
Global
76%

North America
76%

Europe
75%

So, where are IT leaders focusing their efforts to secure data? Blocking of risky apps and gaining visibility into shadow IT were tied for first place, however, in North America, shadow IT visibility was the leading challenge. A core component of CASB, these approaches, along with controlling accidental SaaS file sharing are fundamental to good data hygiene. Also important to organizations is better real-time control over data with DLP and securing motion of this data to unmanaged devices.

Most important use cases of **data protection**



Building a future-proof platform

With the myriad of challenges presented by distributed data and IT complexity, it's to be expected that consolidating vendors ranked on top. It's clear that IT leaders are looking to jettison legacy debt and move toward a more consolidated future built for secure data and hybrid work.

Those who agree that consolidating data protection vendors is a priority

Global	North America	Europe
87%	88%	89%

What does this approach look like? The majority of respondents (with North America leading the pack) are looking to adopt a zero trust approach to data security. The best zero trust approach will be a cloud-delivered model that secures any-to-any connectivity over any network for all users, devices, and apps.

Those who agree that a zero trust approach to data security is critical as remote work increases and data becomes more distributed:

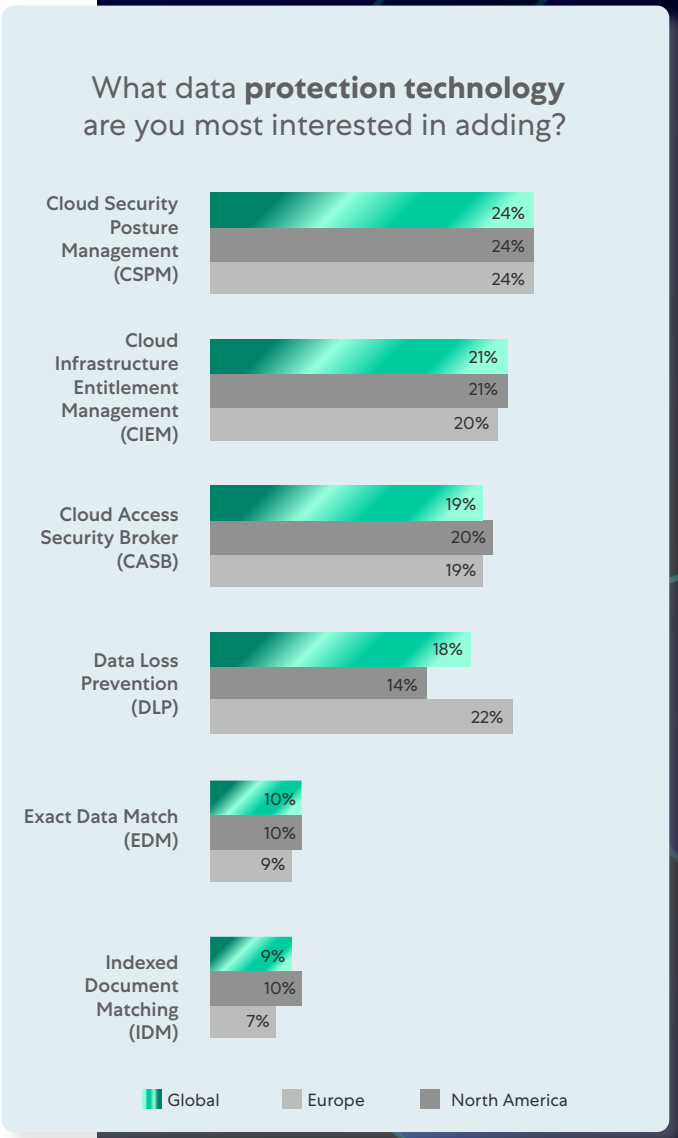
Global	North America	Europe
82%	88%	82%

Focusing on protections that matter

When we look at current weak spots in organizations' defenses, we see that Cloud Security Posture Management (CSPM) and Cloud Infrastructure Entitlement Management (CIEM) both rank at the top. Designed to help quickly spot dangerous misconfigurations or access permissions in SaaS and public clouds, these approaches can help stop cloud breaches in their tracks.

Accounting for nearly 40 percent of responses is the combination of CASB and DLP, which are a fundamental combination for data hygiene. Today's multimode CASBs provide the flexibility and control needed to secure all distributed data.

It's important to call out that all these technologies should ideally be consumed as a cloud service and unified across into a single platform in order to reduce complexity and cost.



Where to Go From Here?

It's clear IT leaders and teams have had to rapidly adapt and evolve over the past 18 months to support and secure an ever-changing remote workforce. The work-from-anywhere trend isn't going anywhere, and it comes with significant complex challenges. Organizations and IT teams will need to continue to innovate, advance, and explore new technologies to stay relevant, competitive, and protected as we move into a new era of the cloud.

For more information on how to improve your data security in the face of hybrid work or the cloud, contact Zscaler.

Learn about Zscaler Data Protection →

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest in-line cloud security platform. Learn more at zscaler.com or follow us on Twitter @zscaler.