netwrix

2019

NETWRIX CLOUD DATA SECURITY REPORT

www.netwrix.com

EXECUTIVE SUMMARY

This is our fourth annual report dedicated to cloud security. With compliance regulations growing tighter and data privacy taking center stage, this year we focused on data security in the cloud. We asked 749 participants from organizations of various sizes located around the world about the kinds of data they store in the cloud, their top concerns about securing that data, the incidents they have experienced and their plans for storing sensitive data in the cloud in the future.

Perhaps the most important take-away from the survey is that organizations are better positioned for success in the cloud if they have insight into what data they have and how it is being used. Specific findings included the following:

- Half of respondents store personally identifying information (PII) of customers and employees in the cloud, but far fewer are willing to store their financial data and intellectual property (IP) there.
- The primary drivers for cloud migration are reducing costs and making data available for remote workers. The appeal of these benefits seems to outweigh security concerns.
- Organizations that perform data discovery and classification (DDC) on their data are much more likely to be able to stick to their cloud budgets.
- 36% of respondents reported being unable to determine the threat actor behind a security incident, up dramatically from just 6% last year.
- One third of organizations that store all their sensitive data in the cloud had security incidents in the past year. Among organizations who had at least one security incident during the preceding 12 months, the number of organizations that use multiple clouds is 20% larger than those who use a single public cloud.
- 75% of organizations that store customer PII in the cloud but did not classify all their data before their cloud migration experienced a security incident.
- Respondents would like to strengthen their cloud data security with strategies like encryption, monitoring of user activity and employee training, but more than half of them are having to manage with the same cloud security budget as last year.
- 21% of organizations have adopted a cloud-first strategy, up from 16% last year. Only 35% intend to become 100% cloud-based within 5 years, with smaller organizations being more likely to do so than mid-size companies and large enterprises.
- Almost half of organizations that store all their sensitive data in the cloud consider or might consider moving their data back on premises. Their reasons include failure to achieve cost savings and security concerns.

DATA IN THE CLOUD

Since cloud security is a broad and complex subject, we decided to start our survey by asking about the types of data organizations choose to store in the cloud. A strong cloud security posture requires organizations to classify data based on its sensitivity and make considered decisions about which data should be moved to the cloud. In this chapter, we will learn what types of data organizations opt to store in the cloud and what types of data they would never migrate there, and the main drivers for their cloud migration.

TYPES OF DATA STORED IN THE CLOUD

The majority of organizations store non-sensitive data in the cloud (57%). On top of that, 50% store personally identifying information (PII) of customers and employees. However, far fewer organizations choose to keep other sensitive information, such as financial data (26%) or intellectual property (IP) (16%), in the cloud (see Diagram 1).

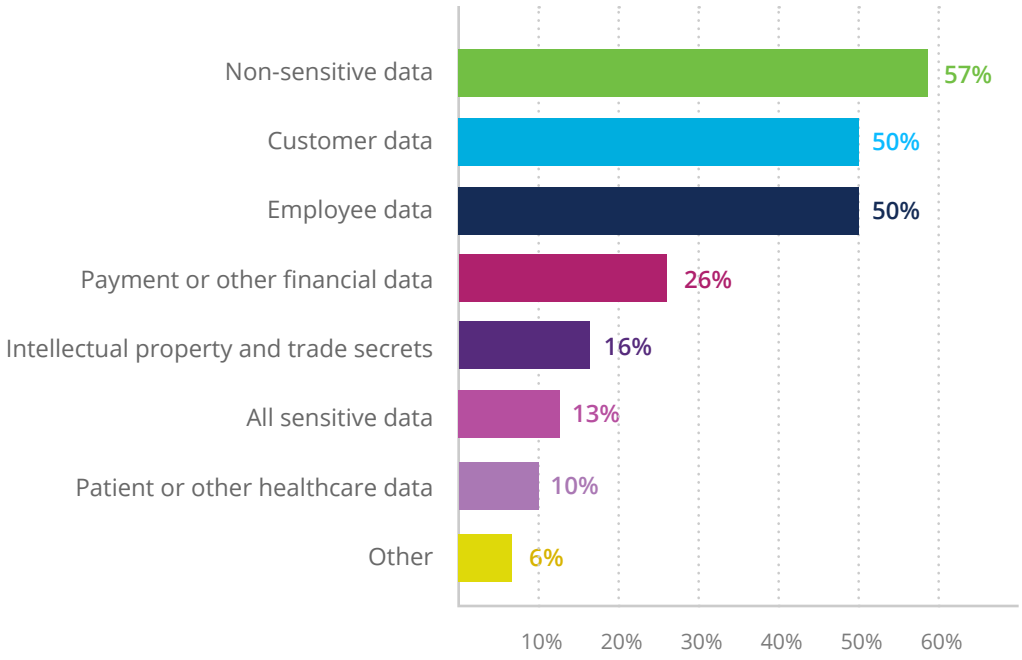


Diagram 1. Types of data organizations store in the cloud

However, the numbers are different for organizations that had at least one security incident during the preceding year: Many more of them report storing sensitive data in the cloud, as shown in Diagram 2.

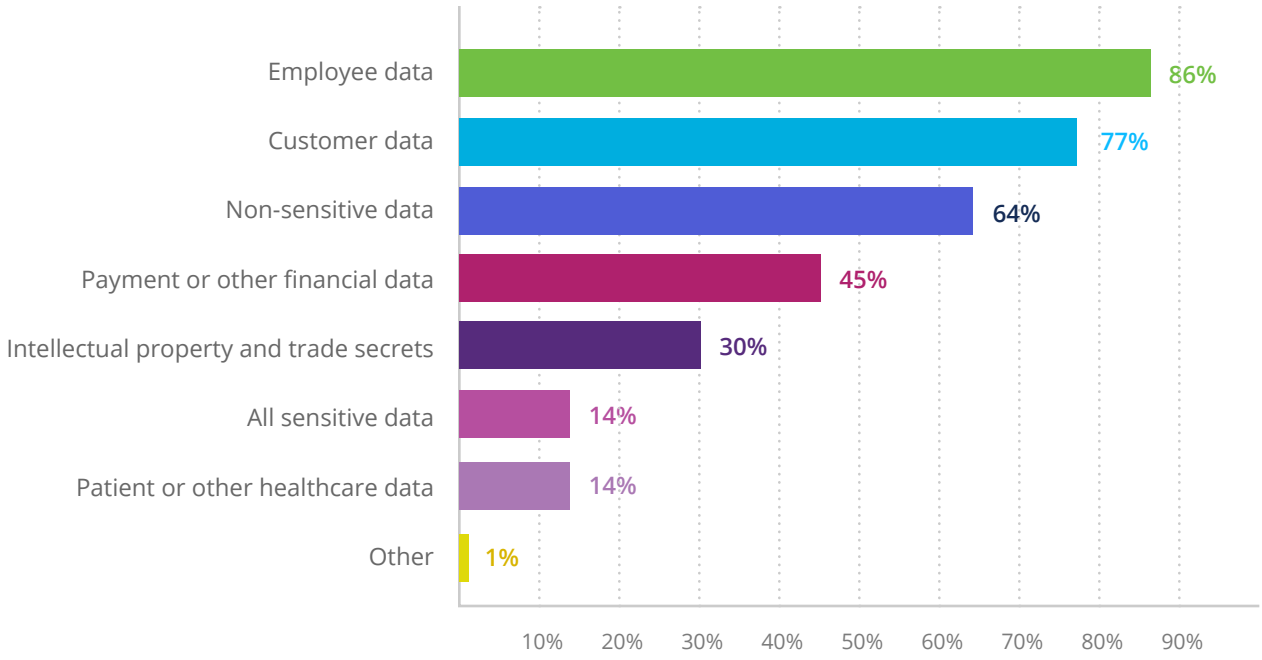


Diagram 2. Types of data stored in the cloud by organizations that had cloud security incidents over the year

However, some organizations that have suffered a breach are careful to never store certain types of data in the cloud, such as IP (41%) and financial data (39%).

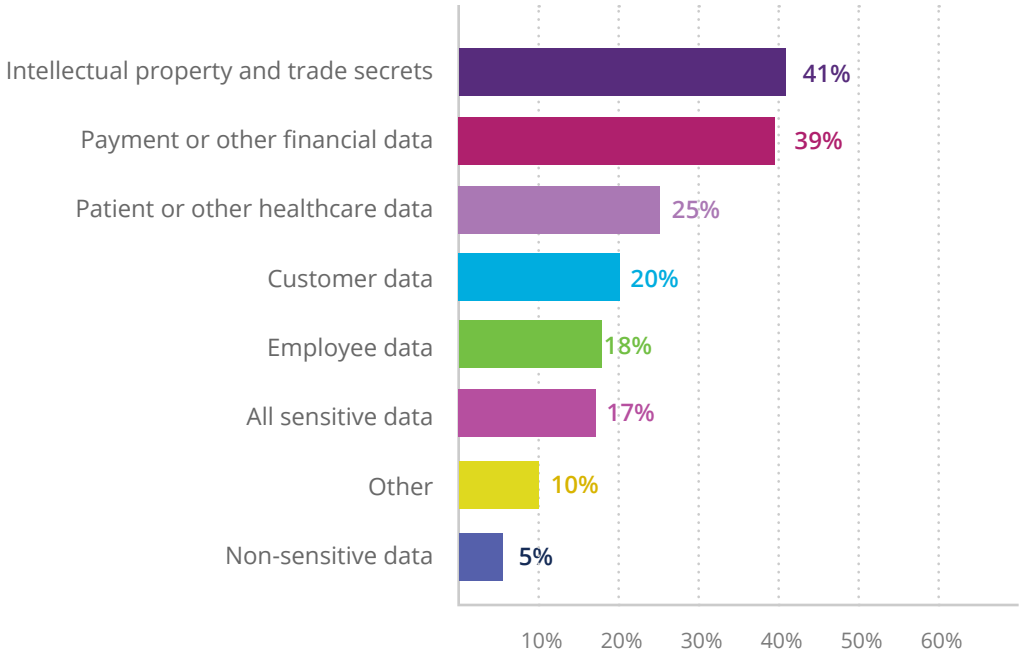


Diagram 3. Types of data that organizations that had cloud security incidents the previous year would never store in the cloud

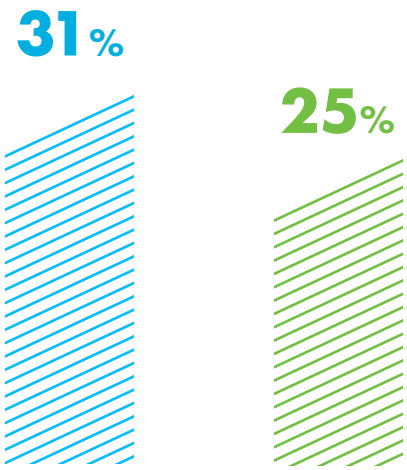
It is worth mentioning that the attitude towards storing PII data in the cloud depends on the organization's size. While 60% of small organizations (with up to 100 employees) store customer PII in the cloud, just 45% of medium and large organizations do.

Size of business	Percentage that store customer data in the cloud
Small (1–100 employees)	60%
Medium (101–1000 employees)	45%
Large (1000+ employees)	45%

Diagram 4. Percentage of organizations that store customer data in the cloud, by size

DRIVERS OF CLOUD MIGRATION

The reasons to move data to the cloud differ from one organization to another, but financial benefits seem to be a huge motivator. For organizations that migrated all their PII to the cloud, the top drivers were cost-efficiency (31%) and making the data available to remote workers (25%). In other words, some organizations are ready to put PII at risk for the sake of profitability and business efficiency.



of organizations that store PII in the cloud are seeking cost savings, and 25% want to make data available to remote workers

The motivations for cloud migration depend on an organization's size. Small organizations said that the leading reason was availability for remote workers (26%), followed by security concerns (24%) and cost-efficiency (22%). This is not a surprise: Smaller businesses often outsource some functions or use remote workers to cut costs, and the cloud enables them to ensure business continuity under those constraints. In addition, cloud providers offer a variety of data protection services and therefore ease the security burden for small organizations that have limited cybersecurity expertise.

Business size	Availability for remote workers	Security concerns	Cost efficiency
Small (1–100 employees)	26%	24%	22%
Medium (101–1000 employees)	26%	16%	30%
Large (1000+ employees)	26%	16%	38%

Diagram 5. Top 3 reasons to store data in the cloud by organization size

Unlike small organizations, more than 30% of medium-sized and large organizations named cost efficiency as the key factor in their decision to move data to the cloud. Indeed, from the enterprise perspective, storing data in the cloud is associated with significant savings on infrastructure and software by reducing the need for on-site servers and staff to manage them.

Another interesting fact revealed by the survey is that organizations that use different types of cloud have different drivers for cloud migration. Quite expectedly, the primary reason for moving data to a private cloud is security concerns (24%), while availability to remote workers (32%) stimulates organizations to consider a public cloud. Organizations start to experiment with multiple public clouds primarily to optimize costs (31%).

Type of Cloud Used	Availability for remote workers	Security concerns	Cost efficiency
Private cloud	20%	24%	22%
Single public cloud	32%	21%	27%
Multiple public clouds	25%	18%	31%

Diagram 6. Top 3 reasons organizations store data in the cloud, by type of cloud infrastructure

The research shows that security is not the main motivation for organizations that opted to store all their data, both sensitive and non-sensitive, in the cloud. For those organizations, the primary drivers were cost efficiency (31%) and simplified access for remote workers to the data (26%).

CLOUD BUDGETS AND SPENDING

As the previous chapter revealed, cost savings are a major driver for cloud adoption. Indeed, cloud providers often highlight how their offerings can help organizations predict spending and stay on budget. We decided to find out whether those benefits are being realized.

The survey findings show that a significant factor in reaping the budget benefits of the cloud is whether the organization performs data discovery and classification (DDC) on their data. Classifying data by its sensitivity and business impact is an essential step, both before cloud migration and as an ongoing process. It enables organizations to keep sensitive data out of the cloud to reduce its exposure, as well as identify redundant, obsolete or trivial (ROT) files that can be deleted to improve data management and control expenses.

Cloud providers oversell the product, so we had to audit what the real costs were over the advantages. We re-negotiated and unraveled convoluted contracts and terminated others early with penalties, which was worth it in the long run.

Security/compliance officer at a mid-size energy organization

In fact, 81% of organizations that classify their data easily meet their monthly/annual cloud budgets, but 73% of those who say they overpay for cloud services do not classify all the data they store in the cloud.

81% of organizations that classify the data they store in the cloud meet their monthly/annual cloud budgets.

Interestingly, organizations that overpay for the cloud often migrated customer and employee data to improve cost efficiency and reduce security risks. However, by neglecting data classification, they failed to achieve either of those goals.

DATA SECURITY IN THE CLOUD

Although cloud providers like Microsoft or Amazon offer much more advanced security services than many small organizations can afford, often they are not enough to protect data stored in the cloud, as illustrated by headlines about breaches due to cloud misconfigurations. Since most of our respondents store sensitive data in the cloud, we dived deeper into the cloud threat landscape to learn about organizations' current concerns and the ways they enforce data protection.

CLOUD SECURITY THREATS

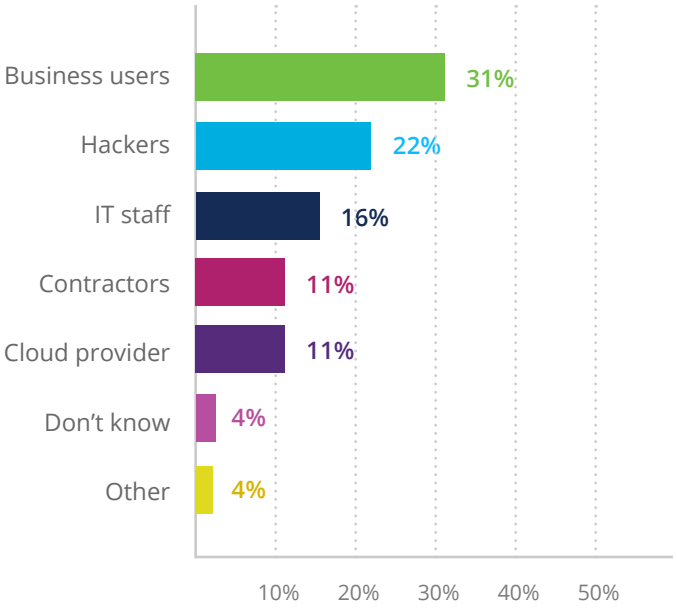


Diagram 7. The top threat to data security in the cloud, according to organizations that had a security incident during the preceding year

We asked organizations that experienced at least one cloud security incident during the preceding year which threat actor represents the biggest risk to data security in the cloud. The majority (58%) chose insiders — either their own business users (31%), members of IT team (16%), or third-party partners and contractors with legitimate access to the internal network (11%). Just 22% chose hackers.

It was surprising that internal IT staff ranked third, at 16%, since these employees are often responsible for the cloud server misconfigurations in the news and their high-level privileges put the company at risk from both malicious and accidental actions. Overall, the list of the top threat actors has not changed much since last year's Netwrix Cloud Security Report.

The top threat actors are the same as last year: business users, hackers, IT staff.

These perceptions about the top threats are correct: Business employees, hackers and IT staff were responsible for most of the incidents that respondents suffered during the preceding year. We were glad to see that most organizations understand who poses the most risk.

36% of organizations could not identify who was at fault for their cloud security incidents, up dramatically from just 6% last year.

However, the ability of organizations to identify the actors responsible for incidents has diminished significantly — 36% of respondents were not able to determine who caused an incident, as opposed to 6% in 2018. This is quite disturbing and demonstrates that organizations do not have enough visibility into their IT infrastructure to conduct effective investigations and learn how to prevent similar incidents in the future.

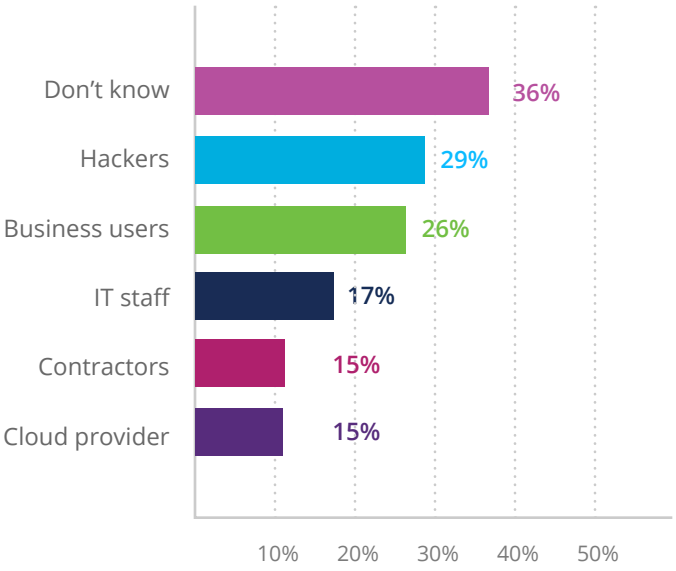


Diagram 8. Threat actors responsible for cloud security incidents during the preceding year

SECURITY INCIDENTS IN THE CLOUD

A third (33%) of respondents that store all their sensitive data in the cloud reported that they had experienced at least one security incident during the preceding 12 months. Security incidents were also experienced by 39% of organizations that store financial data in the cloud, 36% of those who store personal customer data and 35% of those who store healthcare data.

33% of organizations that store all sensitive data in the cloud had security incidents in the past year.

The most common reasons for data security incidents in the cloud were malware (47%), external attack (44%) and accidental errors (36%). Compared to 2018, the number of accidental errors has increased by 14% and the number of malware attacks has increased by 11%, while the number of external attacks has decreased by 20%. This demonstrates that employees' lax attitudes about security have become a bigger problem, which should be tackled by improving control over their activity, conducting security training, and granting privileges and access rights strictly on a need-to-know basis.

The number of accidental errors that resulted in a security incident increased by 14% since our 2018 study.

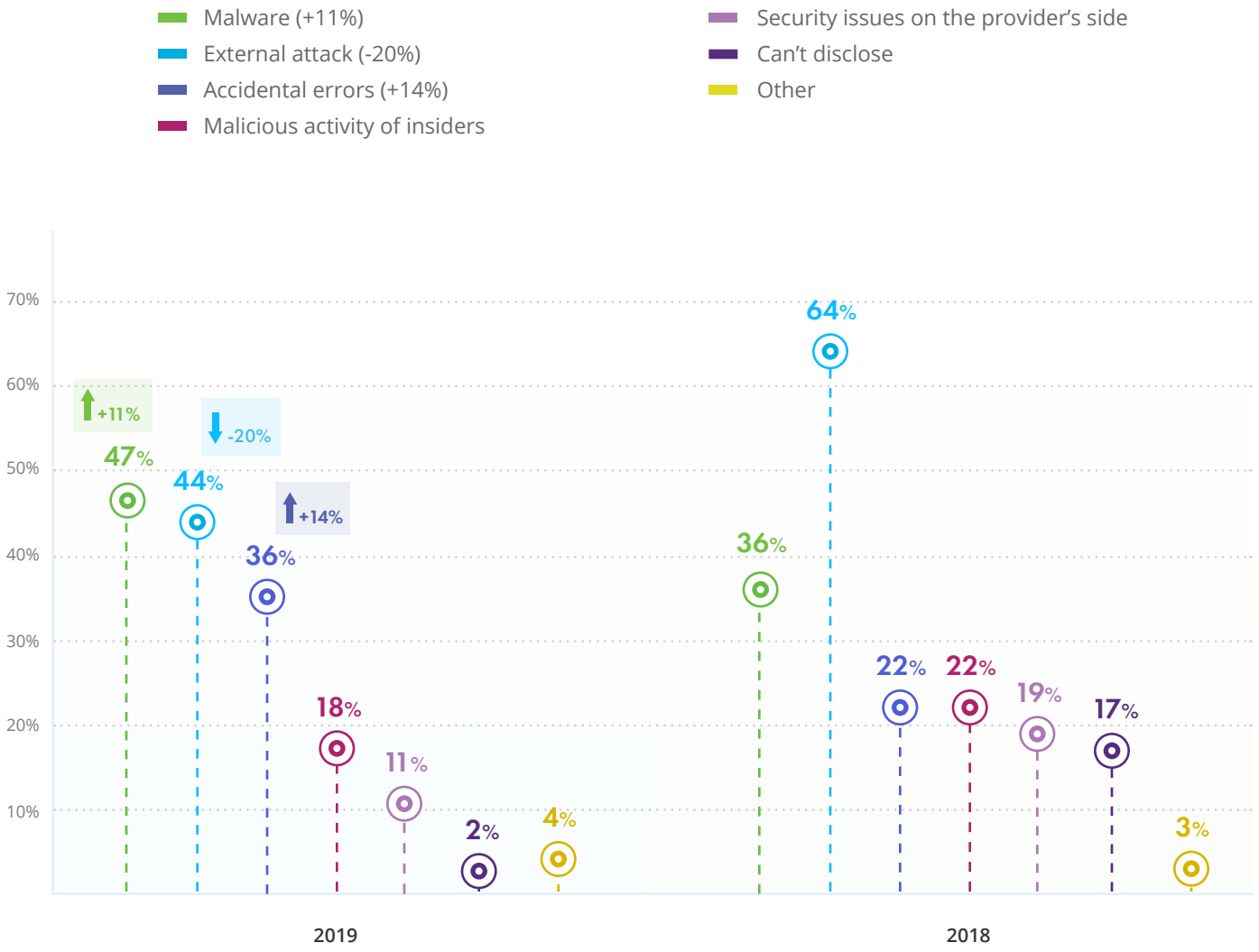


Diagram 9. Types of cloud security incidents during the preceding 12 months

The risk of security incidents is strongly correlated with whether the organization classifies its data: 75% of organizations that store customer PII in the cloud but did not classify all their data experienced at least one security incident — a rate 3.5 times higher than for organizations that did perform data classification. One likely cause is that lack of insight into data hinders IT teams from prioritizing their security efforts on protecting the most critical content.

Among organizations who had at least one security incident during the preceding 12 months, the number of organizations that use multiple clouds is 20% larger than those who use a single public cloud (44% and 24%, respectively). Using multiple clouds complicates security strategy. Without the right tools, it is fairly difficult to manage different cloud identities and have pervasive visibility into what data is stored in each cloud, who has access to it and what happens around it. Moreover, using multiple clouds can increase your attack surface area; an intruder who compromises one account might be able to access all your cloud environments.

CLOUD DATA PROTECTION

The top five measures respondents are taking or plan to take in order to strengthen cloud data security are the following: encrypt data (59%), monitor activity around sensitive data (52%), enforce stricter security policies (51%), adopt or improve data access management (48%), and train employees (43%). These results are quite similar to those from last year's survey.

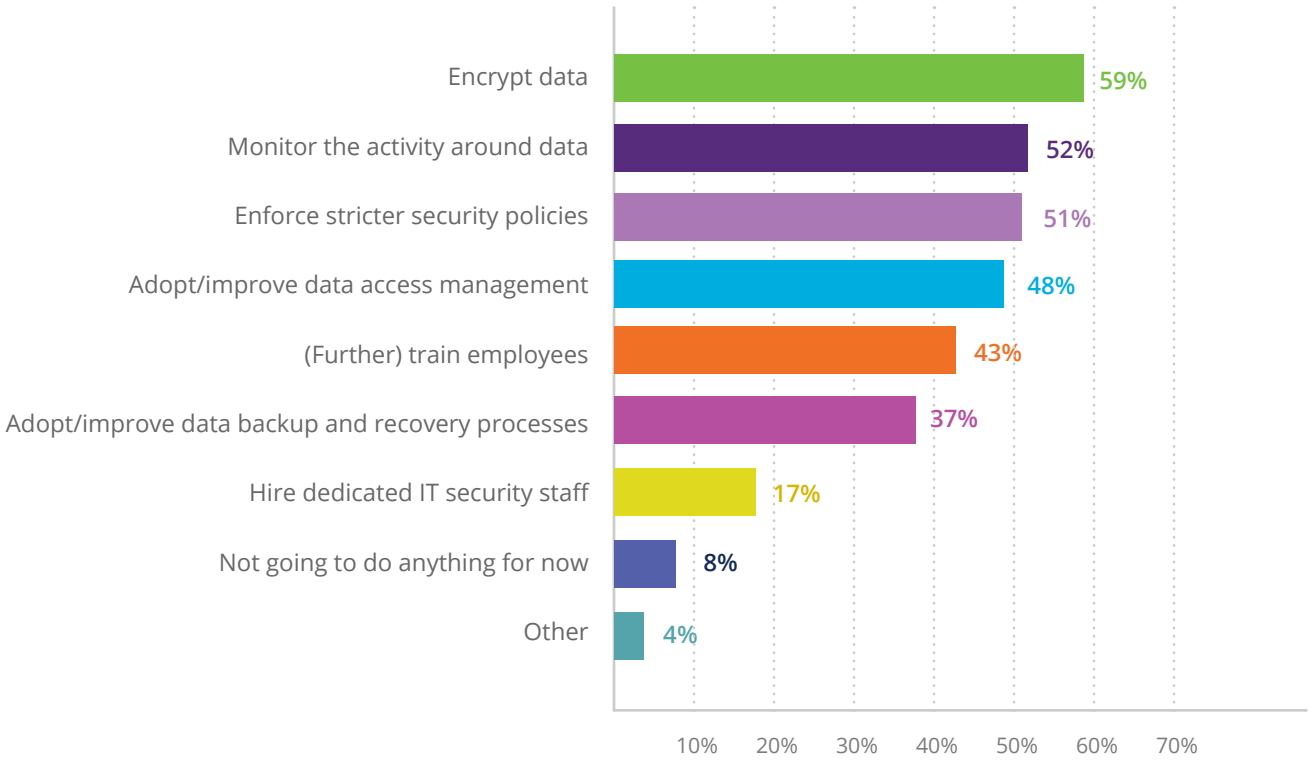


Diagram 10. Measures organizations plan to take to improve data security in the cloud

Do organizations have the resources they need to put their plan into action? Not usually. 55% of organizations report their cloud security budget did not increase in 2019; just 17% were lucky enough to get an annual budget increase of 20%.

Therefore, most IT organizations will have to figure out how to operate within their limited budgets by optimizing and prioritizing their cloud security efforts. Options include investing in solutions that encrypt data or provide visibility into activity around sensitive data, while conducting security training on their own.

Only one person reported a significant budget increase. A public agency in Mexico received 140% more budget for cloud security. They store all their data in the cloud, including IP and personal data of citizens and employees. Hats off to their management for treating sensitive data responsibly!

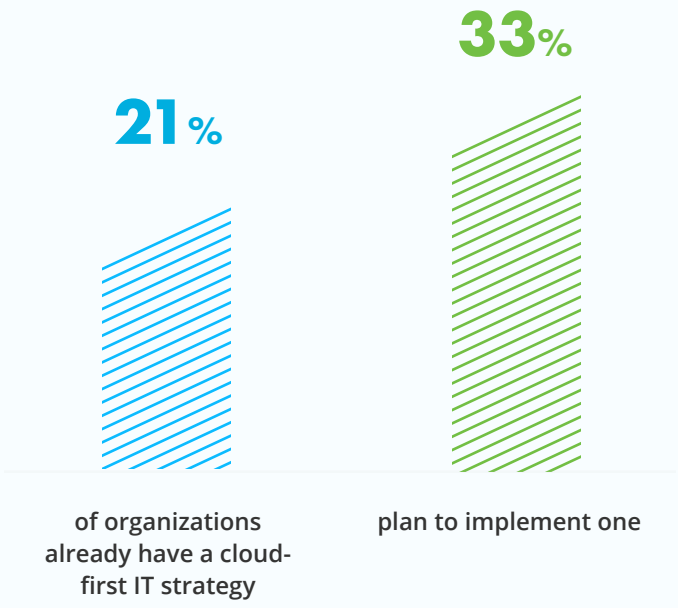
For most organizations (55%), cloud security budgets did not increase in 2019.

PLANS FOR THE FUTURE

Some organizations said that the cloud has not met their expectations and they are considering moving their data back on premises. Other organizations were happier with their experience and are ready to move more of their assets to the cloud or even consider becoming 100% cloud-based.

CLOUD-FIRST STRATEGY

The survey found a small increase in the number of organizations taking a cloud-first approach. 21% of respondents said they consider SaaS as their first option when they plan to adopt new applications or expand current processes, an increase of 5% from 2018.



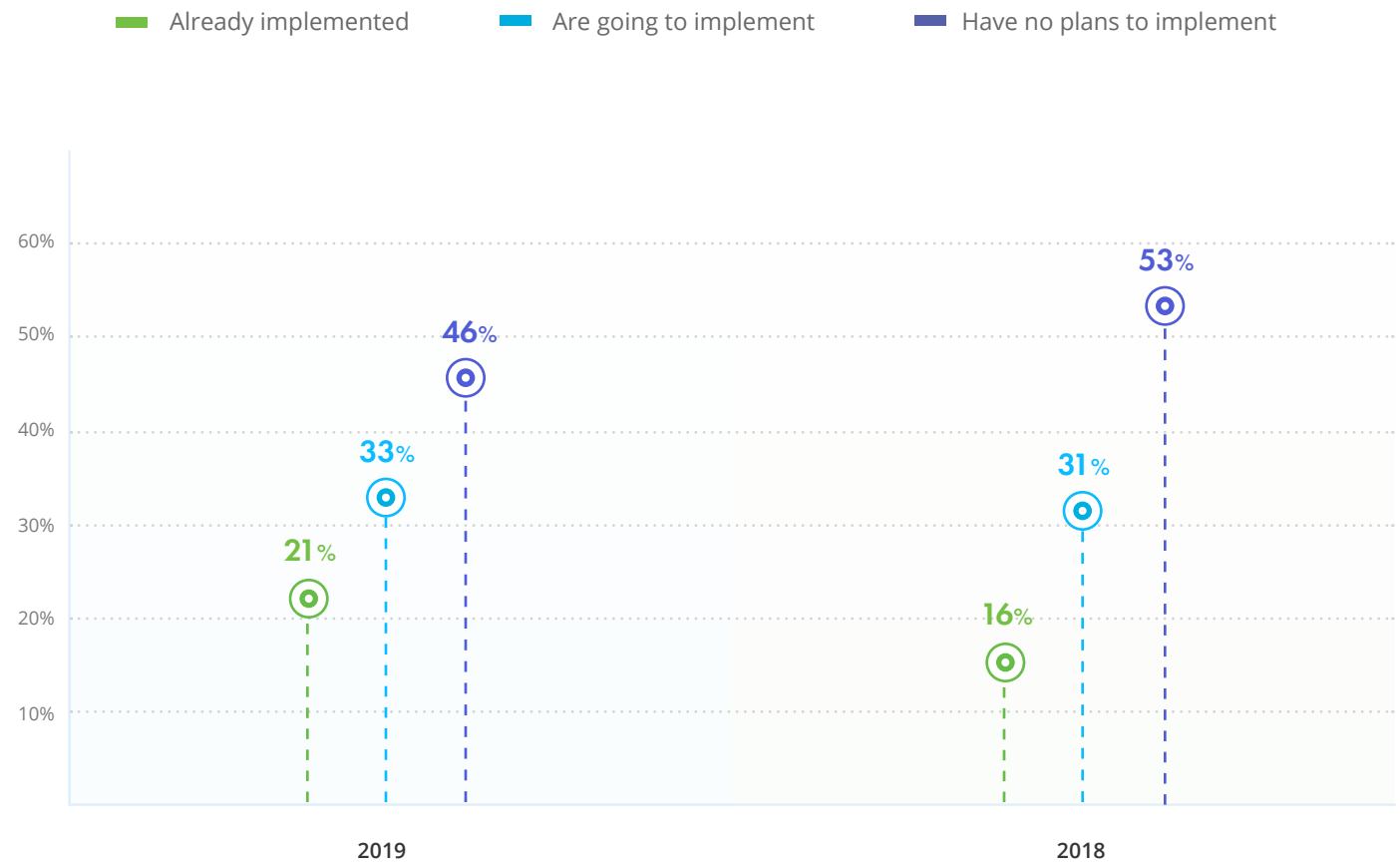


Diagram 11. Readiness to implement a cloud-first strategy

Although 46% of organizations still do not have a cloud-first mindset, there is a positive trend, which suggests that more organizations will move their applications and processes to the cloud in the coming years. Smaller organizations are a bit more likely to implement a cloud-first strategy (37%) than enterprises (35%) and midsize organizations (27%). This is not surprising, given that, as mentioned earlier, small organizations often migrate to the cloud to improve availability for remote workers, security and cost efficiency, and a cloud-first strategy helps them achieve these goals, for example, by replacing more expensive and less efficient on-premises technologies with cheaper and more flexible cloud solutions. In contrast, larger organizations sometimes prefer to leave a substantial part of their infrastructures on premises to have better control over their data.

100% CLOUD

The number of organizations that are ready to move their entire infrastructures to the cloud in the next 5 years remains relatively low. About 28% of organizations are ready to transition to being 100% cloud-based; in 2018, the number was nearly the same (31%). The majority of respondents (65%) stated that they are either unsure about fully moving to the cloud or have no such plans at all.

65%

of respondents are not ready to become 100% cloud-based in the next 5 years.

While the overall attitude towards going "all-cloud" remains conservative, the numbers differ by organization size. Smaller organizations are more likely to move their entire IT infrastructure to the cloud within the next 5 years (35%) than medium-sized organizations (25%) or enterprises (23%). Since the cloud provides the opportunity to stand up an IT infrastructure and secure data without spending a lot of money and resources, it's no wonder that smaller organizations are among the first to consider moving all of their assets to the cloud.

UNCLOUDING (DE-CLOUDING) DATA

As noted earlier, not all organizations are happy with their cloud IT infrastructures. About 48% of respondents who store all their sensitive data in the cloud have considered or might consider moving their data back on premises. The major reasons are concerns about data security (24%) and high cost (22%) in the cloud.

Of those who store all their data in the cloud, 43% would start by moving the personal data of their customers back on premises, and 26% would start with employee information. These findings match one of the major trends in the privacy space — organizations are trying to focus their efforts on securing the personal data on their customers and employees due to tightened compliance regulations and increased attention from the public about the security of their PII.

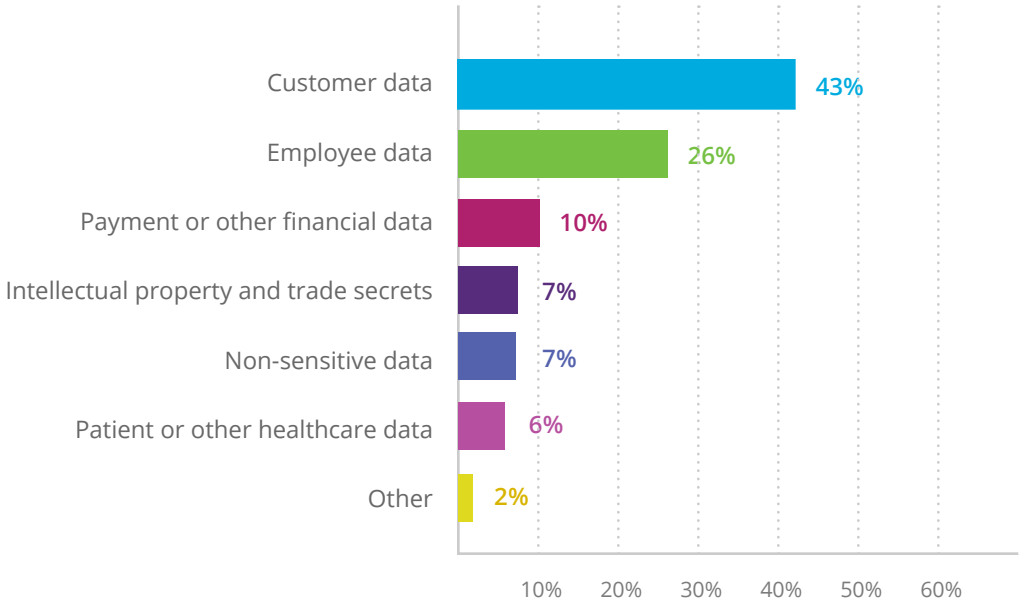


Diagram 12. Types of data that organizations who store all their sensitive data in the cloud would choose to move back on premises first

De-clouding data is often driven by an inability to reach goals. Among organizations that named cost reduction as the major reason to store the PII of their customers and employees in the cloud, 55% have considered or might consider moving this data back on premises. Their reasons include high costs (29%), lack of control (27%) security issues (22%). A similar number of organizations that moved that data to the cloud primarily to improve data security would consider de-clouding their data (54%); their top drivers are security (27%), high cost (23%), reliability and performance issues (16%).

Main reason for cloud migration	Percentage that Would Consider Unclouding	Top Driver
Cost reduction	55%	High costs (29%)
Data security	54%	Poor security (27%)

Diagram 13. How goals for cloud adoption correlate with likelihood of unclouding

One important reason these organizations failed to achieve their goals might have been lack of knowledge about what data they have. With deeper insight into their data, they could have moved only information that was necessary to put in the cloud, gotten rid of stale data, had more control over sensitive content in the cloud and been better able to predict costs.

RECOMMENDATIONS

Adjust your cloud initiatives based on the new privacy regulations.

New privacy laws like the GDPR and the CCPA are forcing organizations to change the ways the store and process sensitive data. Some organizations might think that compliance requires them to move all their PII back on premises, but that's not necessarily true. Rather, since cloud security is a shared responsibility, they need to evaluate the risks to their data, and then move forward on two fronts: On the one hand, they should ask their cloud service providers to add controls that could strengthen data security, such as encryption and data governance. On the other, they should implement their own controls, such as measures to ensure they find all the information they store about a given data subject and delete it if necessary.

Implement controls to investigate security incidents properly.

The survey found that more than a third of respondents were unable to determine who was to blame for a security incident in the cloud. This disturbing fact shows that organizations lack sufficient visibility into their critical systems. To investigate incidents quickly and protect sensitive data against future threats, organizations need to be able to detect, analyze and react to suspicious activities quickly, as well as proactively review access rights and assess vulnerabilities on a regular basis.

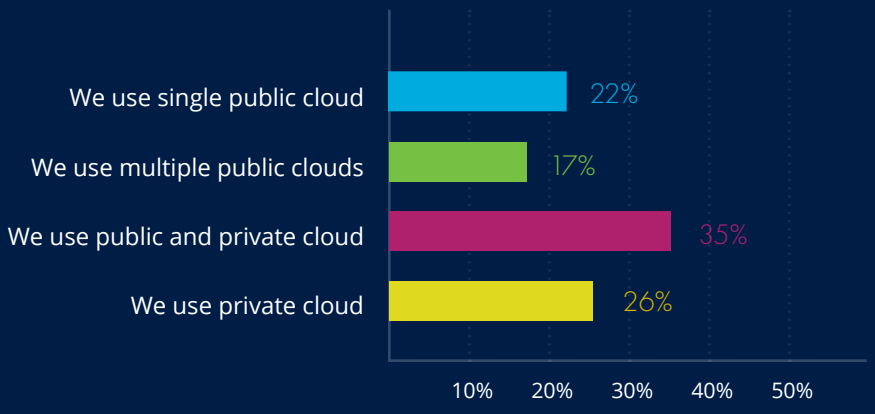
Use data discovery and classification to strengthen your security posture.

Before a migration, DDC helps organizations determine which data to move to the cloud and which to keep on premises. If an organization has already migrated data to the cloud and is concerned about security, DDC will help them decide which data to leave in there and which to move back on premises. Moreover, DDC helps organizations — whether they are on-prem only, cloud-only or hybrid — focus their security efforts on truly important data and choose appropriate controls for different data based on its value and sensitivity.

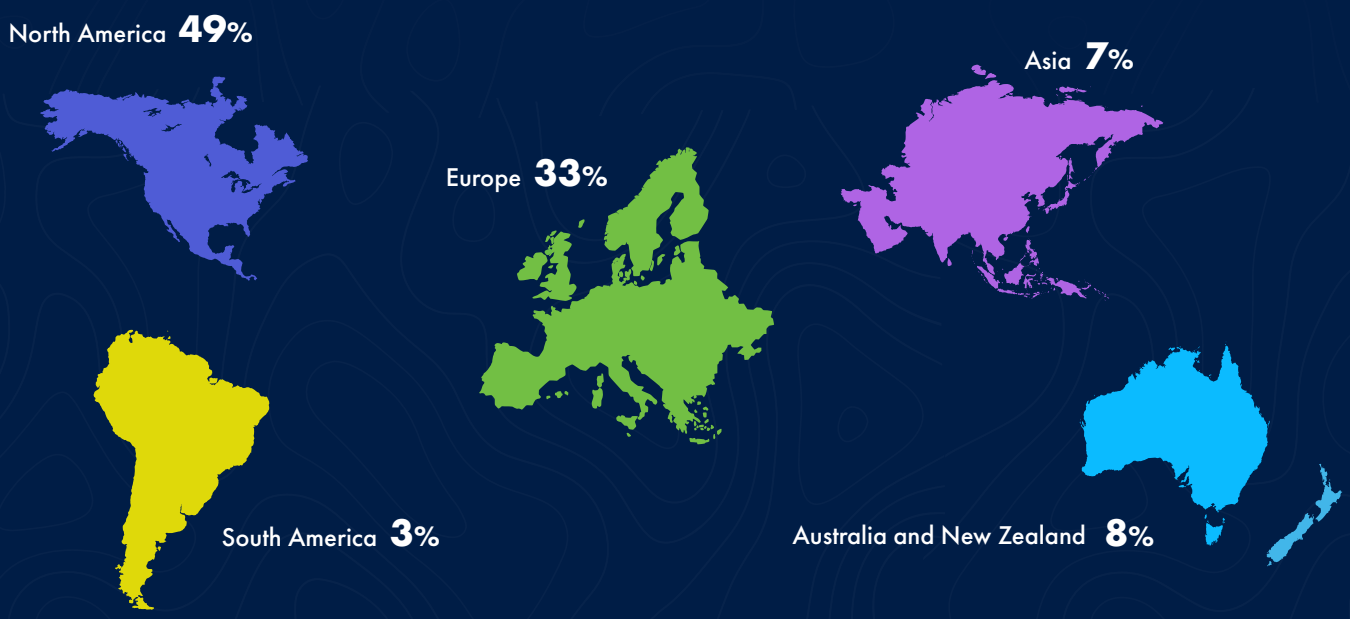
DEMOGRAPHY

749 respondents

TYPE OF CLOUD



GEOGRAPHY



TOP 10 INDUSTRIES

Technology/Managed Services	11%
Technology/Software	11%
Banking & Finance	9%
Health Care	9%
Education	8%
Government	7%
Manufacturing	6%
Consulting	5%
Service	5%
Retail & Wholesale	4%

ORGANIZATION SIZE (GARTNER DEFINITION)

Small Size (up to 100 employees)	34%
Medium Size (101-1000 employees)	36%
Large Size (1000+)	30%

JOB TITLE

System Administrator	37%
IT Manager	24%
CIO/IT Director	12%
Security/Compliance Officer	8%
IT Audit Officer	4%
Consultant	10%
Other (please specify)	5%

ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover up-to-date interests and granular trends' analysis of the industry. For more reports, please visit: www.netwrix.com/go/research

ABOUT NETWRIX

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organizations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers. Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S. For more information, visit www.netwrix.com.

Corporate Headquarters:
300 Spectrum Center Drive, Suite 200, Irvine, CA 92618
Phone: 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

www.netwrix.com/social