netwrix

2021

Cloud Data Security Report

www.netwrix.com

EXECUTIVE SUMMARY

In 2020, many organizations quickly adopted cloud technologies to support the sudden shift to remote work. We have revised our annual Cloud Data Security Report to reflect these unprecedented changes, using a survey of 937 IT professionals worldwide conducted via online questionnaire. This report will help organizations benchmark their security efforts against their peers and better understand the threats to data stored in the cloud.

Key findings include the following:

DATA IN THE CLOUD

Fewer organizations are storing data in the cloud than last year. In 2019, 57% of respondents said they store non-sensitive data in the cloud; now only 46% do. The number storing customer data in the cloud dropped from 50% to 44%.

SECURITY INCIDENTS IN THE CLOUD

Organizations experienced an average of 2.8 security incidents in the past 12 months. The top 3 incident types were phishing (40%), ransomware (24%) and accidental data leakage (17%).

DATA BREACH CONSEQUENCES

For 49% of respondents, security incidents didn't result in any serious consequences. But 28% encountered unplanned expenses to fix security gaps, 11% had to pay compliance fines and 8% believe they lost their competitive edge.

Incidents that included supply chain compromise had the most impact on organizations, including compliance fines (53% of organizations), decrease in new sales (47%), change in senior leadership (24%) and lawsuits (29%).

More than a third (35%) of organizations that suffered data theft by hackers said the incident caused them to lose their competitive edge and/or experience increased customer churn.

INCIDENT DETECTION AND RESPONSE

Top three incidents that organizations typically discover within minutes or hours are phishing and ransomware (86%) and targeted attacks on cloud infrastructure (83%). Data theft by insiders and accidental data leakage took the longest to detect. While 50% of respondents spent minutes or hours to detect insider data theft, another half was unaware of the incident for days, weeks or even months. Accidental data leakage was discovered within minutes or hours only by 39% of organizations, while 61% needed days or weeks to spot the incident.

Data theft and accidental data leakage also resulted in the slowest response. 43% of respondents needed days, weeks or months to respond to data theft by an insider; and 40% of respondents required the same amount of time to respond to hacker attacks. 51% of organizations spent days, weeks, months or even years to resolve accidental data leakage.

Data classification and user activity auditing reduced both detection and response time. The majority of organizations that have both technologies detected and resolved incidents within minutes or hours.

CLOUD DATA SECURITY CHALLENGES

48% of CISOs report that business pressure for rapid digitalization, transformation and growth distracts them from data security.

The top three challenges organizations said they need to overcome are understaffed IT teams (52%), lack of budget (47%) and lack of expertise in cloud security (44%). 51% of large enterprises don't have enough knowledge of cloud security to ensure sensitive data is protected.

UNCLOUDING DATA

62% of organizations are going to remove sensitive data from the cloud or have already done so, in order to improve data security. This is up from 48% in 2019.

CLOUD DATA SECURITY MEASURES

The three cloud security controls that organizations are using are encryption (62%), auditing of user activity (58%) and employee training (58%). In 2019, 59% encrypted data, 52% audited user activity and 51% enforced stricter security policies.

CYBERSECURITY SPENDING AND CLOUD SECURITY BUDGET

The pandemic had no impact on cybersecurity spending and priorities for 21% of organizations. 36% of respondents said they had to change their priorities, but still had to act within the existing budget. Only 24% of organizations reported a spending increase.

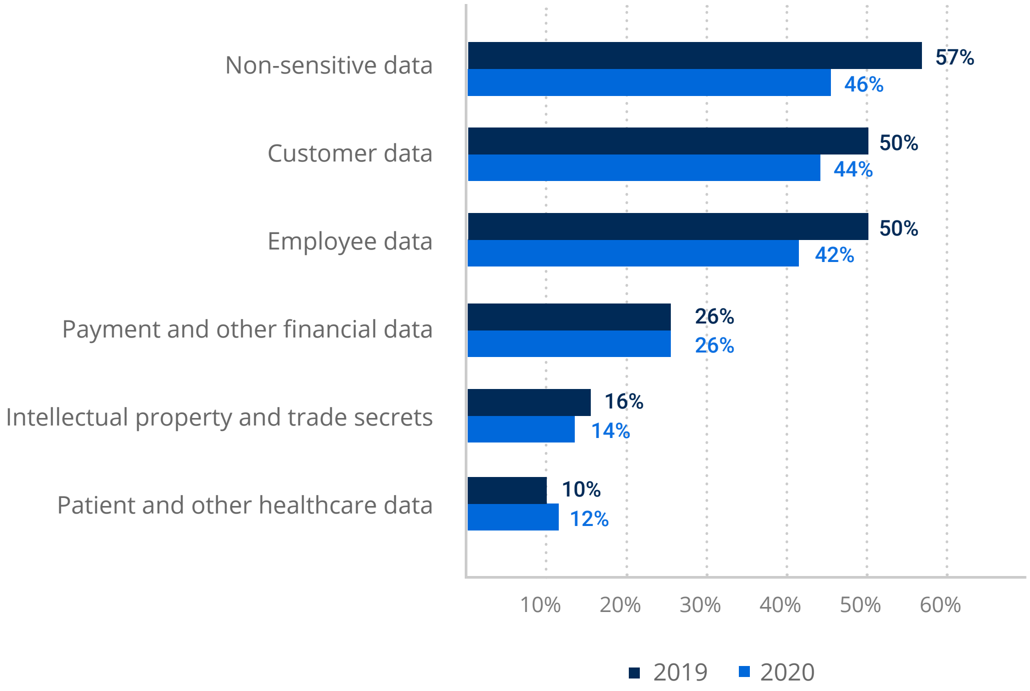
On average, organizations allocate 27% of their cybersecurity budget to cloud security.

DATA IN THE CLOUD

Our research last year found that many organizations (57%) were storing non-sensitive data in the cloud. Given the dramatic increase in remote work in 2020, we expected even more organizations to store this data in the cloud. However, it decreased considerably, to just 46%. The number of organizations storing customer and employee data in the cloud also dropped, though less dramatically.

For other types of data, the percentage didn't change much. It seems that after some organizations dipped their toes into the cloud by putting sensitive and non-sensitive data there, they reassessed their risks and needs and pulled it back.

Types of data organizations store in the cloud



54% of organizations that store customer data in the cloud had security incidents in the past 12 months, compared to 77% in the previous year .

SECURITY INCIDENTS IN THE CLOUD

While we would like to compare this year's survey results to the previous years, it is impossible because we reshaped several questions and offered our respondents more detailed options to choose from. We felt that the previous questions were not reflective of real-world use cases and the results didn't provide actionable information to help organizations build stronger cybersecurity strategies to protect data stored in the cloud. In particular, we made the following changes:

- "External attack" was broken into multiple types of incidents, such as phishing, targeted attacks on infrastructure, account compromise, data loss, data theft and supply chain compromise.
- "Accidental errors" was narrowed to "accidental data leakage".
- "Malicious activity of insiders" was more clearly defined as "data theft by insiders".

Phishing was the most commonly experienced incident, followed by ransomware. Accidental data leakage was next, which is not surprising since it can happen easily, especially if data is stored online.

Most common cloud security incidents

Phishing attacks	40%
Ransomware or other malware attacks	24%
Accidental data leakage	17%
Targeted attacks on cloud infrastructure	16%
Account compromise	16%
Data loss	13%
Data theft by insiders	10%
Data theft by hackers	7%
Supply chain compromise	6%

Larger companies were more likely to suffer external attacks, such as phishing, ransomware and targeted attacks on cloud infrastructure. More of them also reported accidental data leakage and of account compromise, which is to be expected because they simply have more users. Conversely, larger enterprises were less prone to insider data theft. Perhaps this is because they have more advanced activity monitoring, more detailed employment contracts and better cybersecurity education for users.

Cloud security incidents by organization size

	SMALL (1–100 employees)	**MEDIUM** (101–1000 employees)	**LARGE** (1000+ employees)
Phishing attacks	30%	38%	52%
Ransomware or other malware attacks	15%	23%	35%
Accidental data leakage	15%	14%	21%
Targeted attacks on cloud infrastructure	13%	14%	21%
Account compromise	13%	15%	20%
Data loss	14%	11%	15%
Data theft by insiders	12%	9%	9%
Data theft by hackers	6%	4%	12%
Supply chain compromise	6%	2%	11%

Organizations experienced an average of 2.8 cloud security incidents in the past 12 months.

DATA BREACH CONSEQUENCES

Not all security incidents do the same amount of harm. Almost half of respondents said the security incidents they suffered did not result in any issues. 28% of respondents encountered unplanned expenses to fix security gaps, and 11% of organizations were liable for compliance fines.

Interestingly, large enterprises were more likely to include costs to fix security gaps, and they were also more likely to lose a C-level executive: **Every tenth enterprise had to change senior leadership as part of their data breach response**.

Most common data breach consequences

No issues	49%
Unplanned expenses to fix security gaps	28%
Compliance fines	11%
Loss of competitive edge	8%
Customer churn	8%
Decrease in new sales	8%
Decrease in company valuation	7%
Change in senior leadership	6%
Lawsuits	4%

Data breach consequences by organization size

	SMALL (1–100 employees)	**MEDIUM** (101–1000 employees)	**LARGE** (1000+ employees)
No issues	55%	55%	38%
Unplanned expenses to fix security gaps	22%	28%	35%
Compliance fines	11%	7%	13%
Loss of competitive edge	6%	8%	11%
Customer churn	9%	8%	8%
Decrease in new sales	8%	6%	10%
Decrease in company valuation	7%	4%	10%
Change in senior leadership	3%	5%	10%
Lawsuits	6%	1%	5%

IMPORTANT NOTE

We are unable to identify with 100% accuracy which incidents led to which consequences because a data breach often involved several attack patterns (e.g., a phishing attack leads to account compromise, which results in data theft). Accordingly, in this report, we will not be saying things like “accidental data leakage led to unplanned expenses in 62% of cases” but rather “cloud security incidents that involved accidental data leakage led to unplanned expenses in 62% of cases.”

We were surprised that incidents that included supply chain compromise had the most impact on organizations. They resulted in compliance fines (53% of organizations), decrease in new sales (47%), change in senior leadership (24%) and lawsuits (29%) — all of which were the highest results across all incident types. Security incidents that involved insider data theft negatively impacted company valuation for 33% of organizations, while data theft by hackers led to customer churn and loss of competitive edge (35% each). And finally, human errors or incidents that involved accidental data leakage required 62% of respondents to obtain budget to address the associated security gaps.

Cloud data breach consequences by incident type

- 🟦 Targeted attacks on cloud infrastructure
- 🟩 Phishing attacks
- 🟪 Ransomware
- 🔹 Supply chain compromise
- 🟣 Insider data theft
- 🟨 Hacker data theft
- 🟥 Accidental data leakage
- ▩ Account compromise
- 🟧 Data loss

	🟦	🟩	🟪	🔹	🟣	🟨	🟥	▩	🟧
No issues	23%	35%	27%	12%	11%	10%	13%	21%	17%
Unplanned expenses to fix security gaps	51%	50%	58%	47%	59%	60%	62%	56%	50%
Compliance fines	33%	17%	24%	53%	26%	40%	29%	26%	36%
Loss of competitive edge	26%	12%	15%	29%	26%	35%	22%	21%	25%
Customer churn	28%	11%	15%	18%	15%	35%	22%	14%	25%
Decrease in new sales	26%	7%	15%	47%	19%	30%	16%	23%	17%
Decrease in company valuation	23%	10%	13%	24%	33%	25%	16%	14%	25%
Change in senior leadership	16%	9%	9%	24%	15%	20%	18%	16%	19%
Lawsuits	12%	5%	7%	29%	11%	25%	4%	9%	11%

INCIDENT DETECTION AND RESPONSE

We asked our respondents to estimate how much time their organizations needed to discover and respond to the cloud security incidents they suffered in the past 12 months.

AVERAGE DETECTION TIME

We were fairly surprised at how quickly organizations were able to spot incidents — in the majority of cases, respondents needed only hours to detect the incident, which is actually not that bad. Phishing and ransomware were the easiest to detect; 86% spotted it in minutes or hours. Organizations were also able to spot targeted attacks on cloud infrastructure fairly quickly (83% within minutes or hours).

However, data theft by insiders and accidental data leakage were far more problematic. According to our research, 50% of respondents needed days, weeks or months to detect insider data theft, and 61% admitted that it took them days or weeks to spot accidental data leakage.

Some organizations also struggled to uncover data theft by hackers. It is the only incident type that took years to detect; 5% of respondents reported this.

It is important to note that all incidents we have just talked about are associated with data and its overexposure. Organizations need to ensure they can track what users are doing with data and get alerts if it is improperly accessed or shared so they can take action immediately.

Time to detect security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Targeted attacks on cloud infrastructure	32%	51%	15%	2%	0%	0%
Phishing attacks	44%	42%	13%	1%	0%	0%
Ransomware or other malware attacks	35%	51%	9%	5%	0%	0%
Supply chain compromise	23%	53%	18%	0%	6%	0%
Data theft by insiders	23%	27%	27%	19%	4%	0%
Data theft by hackers	16%	53%	21%	0%	5%	5%
Accidental data leakage	16%	23%	47%	14%	0%	0%
Account compromise	20%	49%	24%	7%	0%	0%
Data loss	23%	42%	29%	6%	0%	0%

10%

of small organizations required months to detect data theft by insiders.

25%

of medium organizations needed years to detect data theft by hackers.

10%

of enterprises took months to detect supply chain compromise.

IMPACT OF DATA CLASSIFICATION AND ACTIVITY AUDITING ON DETECTION SPEED

Data classification enables organizations to tag each sensitive file so they can improve control over where data is stored and who can access it. This technology significantly improved the speed of discovery for four incident types: data theft by insiders, data theft by hackers, accidental data leakage and data loss. Organizations who classified their data were able to spot these incidents in minutes or hours, while other organizations needed days, weeks or even months.

Impact of data classification on speed of incident detection

	CLASSIFY DATA	DON'T CLASSIFY DATA
Data theft by insiders	58% discovered in minutes or hours	55% discovered in days or weeks
Data theft by hackers	75% discovered in minutes or hours	60% discovered in days or months
Accidental data leakage	60% discovered in minutes or hours	85% discovered in days or weeks
Data loss	53% discovered in hours	56% discovered in days

Auditing of user activity improved detection time in a similar way for five incident types: supply chain compromise, data theft by insiders, data theft by hackers, accidental data leakage and account compromise.

Impact of user activity auditing on speed of incident detection

	AUDIT USER ACTIVITY	DON'T AUDIT USER ACTIVITY
Supply chain compromise	75% discovered in minutes or hours	69% discovered in days or weeks
Data theft by insiders	64% discovered in minutes or hours	58% discovered in days, weeks or months
Data theft by hackers	78% discovered in minutes or hours	66% discovered in weeks or months
Accidental data leakage	58% discovered in minutes or hours	70% discovered in days or weeks
Account compromise	76% discovered in minutes or hours	67% discovered in days or weeks

We highly recommend deploying both technologies to improve incident discovery time and mitigate risk.

Organizations that both classify data and audit user activity are 1.5 times more likely to discover incidents in minutes.

AVERAGE RESPONSE TIME

Managing the aftermath of a security incident takes organizations longer than incident detection. The best results were for phishing — 82% of organizations resolved the incident in minutes or hours. Next were targeted attacks and data loss, which 69% resolved in minutes or hours.

At the other end of the spectrum were incidents related to accidental data leakage, which 51% of organizations needed days, weeks, months or even years to resolve. 43% of respondents needed days, weeks or months to respond to insider data theft and 40% needed that long to respond to hacker attacks. We would also like to highlight that 15% of organizations needed months to handle data theft by hackers, which is the worst result across all incident types we analyzed.

Interestingly, **data theft and accidental data leakage required the longest time to both detect and respond to**. Organizations need to ensure they can promptly identify unauthorized data access or data sharing and develop effect response processes to minimize the damage, reduce the cost of data breaches, and find and fix the root cause to prevent similar incidents in the future.

Time to respond to security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Targeted attacks on cloud infrastructure	20%	48%	20%	10%	2%	0%
Phishing attacks	41%	41%	15%	2%	1%	0%
Ransomware or other malware attacks	26%	39%	27%	6%	2%	0%
Supply chain compromise	18%	46%	24%	12%	0%	0%
Data theft by insiders	26%	31%	27%	12%	4%	0%
Data theft by hackers	15%	45%	20%	5%	15%	0%
Accidental data leakage	9%	40%	33%	14%	2%	2%
Account compromise	29%	34%	27%	5%	5%	0%
Data loss	19%	49%	20%	6%	6%	0%

20%

of small organizations spent months to resolve data theft by hackers.

25%

of medium organizations needed weeks to resolve data theft by either hackers or employees.

18%

of large enterprises required months to resolve data theft by hackers, and 13% needed that long for data theft by insiders.

IMPACT OF DATA CLASSIFICATION AND ACTIVITY AUDITING ON RESPONSE SPEED

Data classification enabled organization to respond faster to five types of incidents: ransomware, data theft by insiders, data theft by hackers, accidental data leakage and data loss. Data classification enables organizations to determine which incidents involve critical data and need urgent attention, so they can prioritize recovery initiatives. As a result, organizations with data classification in place were able to resolve these incidents in minutes or hours, while other organizations needed days, weeks or months.

Impact of data classification on speed of incident response

	CLASSIFY DATA	DON'T CLASSIFY DATA
Ransomware or other malware attacks	72% resolved in minutes or hours	50% resolved in days or weeks
Data theft by insiders	66% resolved in minutes or hours	55% resolved in days or weeks
Data theft by hackers	67% resolved in minutes or hours	80% resolved in days, weeks or months
Accidental data leakage	70% resolved in minutes or hours	63% resolved in days or weeks
Data loss	74% resolved in minutes or hours	64% resolved in days or weeks

Auditing of user activity improved response speed for seven incident types: targeted attacks, ransomware, data theft by insiders, data theft by hackers, accidental data leakage, account compromise and data loss. Having an audit trail enabled the majority of organizations to respond to these incidents in minutes or hours, while the other organizations required day, weeks or months.

Impact of user activity auditing on speed of incident response

	AUDIT USER ACTIVITY	DON'T AUDIT USER ACTIVITY
Targeted attacks on cloud infrastructure	75% resolved in minutes or hours	63% resolved in days or weeks
Ransomware or other malware attacks	72% resolved in minutes or hours	59% resolved in days or weeks
Data theft by insiders	73% resolved in minutes or hours	61% resolved in days or weeks
Data theft by hackers	60% resolved in minutes or hours	74% resolved in days or weeks
Accidental data leakage	55% resolved in minutes or hours	59% resolved in days or weeks
Account compromise	65% resolved in minutes or hours	60% resolved in days, weeks or months
Data loss	61% resolved in minutes or hours	70% resolved in days or weeks

CLOUD DATA SECURITY CHALLENGES

The top data security challenges named by survey respondents were lack of IT staff (52%), lack of budget (47%) and lack of cloud security expertise (44%). Employee negligence was named by 38% of respondents, but just 17% chose malicious actions of insiders as an issue. This finding reflects reality, since only 10% of organizations reported data theft by employees.

One in four respondents said that business executives put pressure on the IT team to drive rapid digital transformation or growth to the detriment of data security. This problem is especially critical for **CISOs — 48% note that the business's desire for growth hinders efforts to ensure data security in the cloud**.

Top challenges to ensuring data security in the cloud

52%	IT/security team being understaffed
47%	Lack of budget
44%	Lack of expertise in cloud security
38%	Employee negligence
28%	Lack of visibility into sensitive data in the cloud
26%	Business pressure for rapid digitalization, transformation or growth
25%	Inconsistent tools and processes due to multiple workloads across different cloud platforms
17%	Malicious actions by employees
16%	Inability to secure end points

Top pains for CISOs

73%	Lack of IT/security personnel
48%	Business pressure for rapid digitalization, transformation or growth
41%	Employee negligence

Top pains for CIOs

68%	Lack of budget
48%	Lack of IT personnel
48%	Lack of expertise

The same challenges were in the top three spots regardless of organization size. What surprised us is that half of enterprise organizations listed lack of cloud security knowledge as a cloud security challenge. Clearly, their complex infrastructures and wider use of cloud technologies require IT pros with advanced skills; if you know how to handle this and are looking for a job, you know what to do.

Top challenges to ensuring data security in the cloud by organization size

	SMALL (1–100 employees)	**MEDIUM** (101–1000 employees)	**LARGE** (1000+ employees)
IT/security team being understaffed	45%	62%	47%
Lack of expertise in cloud security	40%	41%	51%
Lack of budget	44%	48%	48%
Employee negligence	40%	33%	41%
Malicious actions by employees	18%	16%	16%
Inconsistent tools and processes due to multiple workloads across different cloud platforms	27%	24%	22%
Inability to secure end points	14%	15%	18%
Lack of visibility into sensitive data in the cloud	27%	31%	26%
Business pressure for rapid digitalization, transformation or growth	26%	22%	31%

CLOUD DATA SECURITY CHECKLIST

The most popular cloud security controls that organizations already have in their arsenal are encryption (62%), auditing of user activity (58%) and employee training (58%). These measures were also listed as the top controls for cloud security in our 2019 survey. Interestingly, in 2019, 37% of respondents said they had adopted or improved data backup strategies; in 2020, 58% of organizations say they already do backups and 24% plan to do them in the future. Also, the overwhelming majority of respondents either already classify sensitive data in the cloud (49%) or plan to implement this control in the future (31%). The most unpopular measure in the batch is cloud access security brokers — 40% don't plan to implement this technology at all.

Measures to protect data in the cloud

	Already do	Plan to do	Don't plan to do
Encryption	62%	25%	12%
Auditing of user activity	58%	29%	12%
Cloud backups	58%	24%	18%
Employee training	58%	31%	11%
Multifactor authentication	57%	31%	13%
Review of access rights (attestation)	54%	34%	12%
Data classification	49%	31%	20%
Remove sensitive data from the cloud	35%	27%	38%
Cloud access security broker	27%	33%	40%

UNCLOUDING (DE-CLOUDING) DATA

In the last year's research, we noted that not all organizations were happy with their cloud infrastructures. About 48% of respondents had moved or planned to move sensitive data back on premises to improve data security. In 2020, despite the surge in cloud adoption due to the need to support remote work, the share of organizations that have already removed sensitive data from the cloud or are planning to do so increased to 62%.

The enterprise sector is more prone to removing data from the cloud; 40% have already unclouded some of their sensitive data and 30% plan to do so. In contrast, almost half of medium organizations have no plans to remove sensitive data from the cloud.

Measures to protect data in the cloud by organization size

Small (1-100 employees)

	Already do	Plan to do	Don't plan to do
Cloud backups	58%	24%	18%
Multifactor authentication	55%	30%	15%
Employee training	54%	35%	11%
Encryption	52%	33%	15%
Review of access rights (attestation)	49%	35%	16%
Auditing of user activity	45%	41%	14%
Data classification	43%	30%	27%
Remove sensitive data from the cloud	36%	25%	39%
Cloud access security broker	26%	25%	49%

Medium (101-1000 employees)

	Already do	Plan to do	Don't plan to do
Encryption	62%	24%	14%
Cloud backups	58%	19%	23%
Employee training	58%	29%	13%
Auditing of user activity	57%	29%	14%
Multifactor authentication	53%	31%	16%
Review of access rights (attestation)	50%	39%	11%
Data classification	44%	37%	19%
Remove sensitive data from the cloud	28%	26%	46%
Cloud access security broker	26%	37%	38%

Large (1000+ employees)

	Already do	Plan to do	Don't plan to do
Auditing of user activity	74%	18%	8%
Encryption	73%	20%	7%
Review of access rights (attestation)	63%	28%	9%
Multifactor authentication	62%	31%	7%
Employee training	61%	29%	10%
Data classification	59%	26%	15%
Cloud backups	58%	29%	13%
Remove sensitive data from the cloud	40%	30%	30%
Cloud access security broker	29%	38%	33%

92%

of large organizations either already audit user activity or plan to do so in order to secure data in the cloud. It is the top cloud security control in the enterprise sector.

64%

of CISOs classify data in the cloud and 27% plan to implement this control in the future.

100%

of CIOs either already conduct employee security training or plan to do so.

CYBERSECURITY AND CLOUD SECURITY BUDGETS

When we asked organizations how the pandemic changed their cybersecurity budgets, only 11% said that their cybersecurity budget has decreased; 24% reported that it grew. More than a third (36%) of organizations say that the pandemic forced them to change their security priorities while staying within their existing budget.

Enterprises were among the lucky ones — 30% of large organizations reported an increase in cybersecurity spending, which is the highest result compared to other organizational sizes.

Impact of the pandemic on cybersecurity spending

36%	Spending stayed the same but priorities changed
24%	Spending increased
21%	Spending and priorities stayed the same
11%	Spending decreased

Impact of the pandemic on cybersecurity spending by organization size

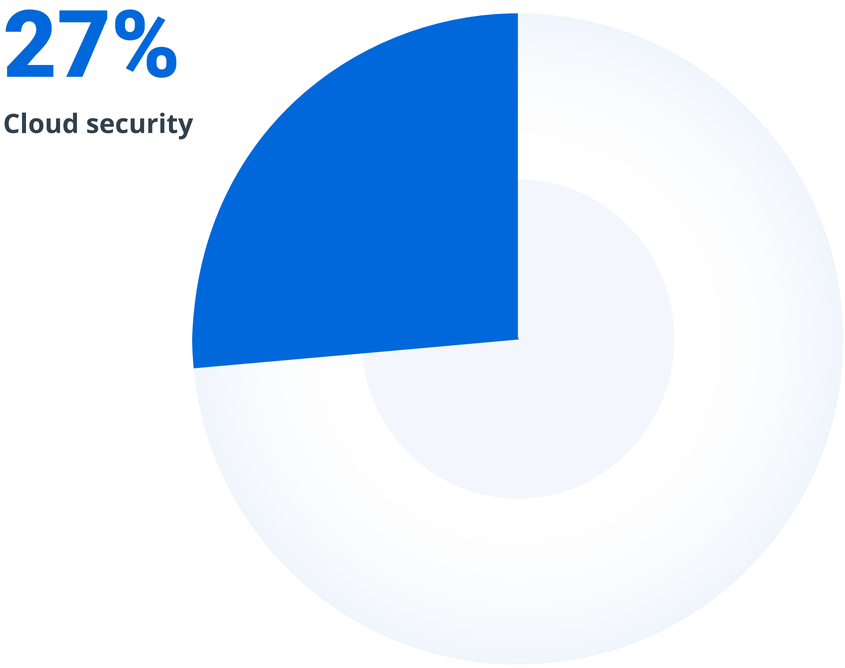
	SMALL (1–100 employees)	**MEDIUM** (101–1000 employees)	**LARGE** (1000+ employees)
Spending has stayed the same, but priorities changed	39%	35%	34%
Spending increased	17%	24%	30%
Spending and priorities stayed the same	26%	20%	16%
Spending decreased	8%	14%	12%

Every second CISO had to review cybersecurity priorities due to the pandemic.

CYBERSECURITY BUDGET DISTRIBUTION

Regardless of size, organizations reported that they allocated more than a quarter of their total cybersecurity budget to cloud security this year.

Portion of cybersecurity budget allocated to cloud security



RECOMMENDATIONS

Continuously audit user activity and classify data to speed incident detection.

The overwhelming majority of respondents that audit user activity and classify their data were able to detect incidents in minutes or hours, while the other organizations needed days, weeks or months. Indeed, having broad visibility into what data the organization stores and what is happening around it not only speeds issue detection, but enables organizations to find and fix security gaps before they suffer a breach.

Automate and/or delegate to do more with less.

Organizations' top three challenges to securing data in the cloud lie in lack of staff, financial resources and expertise. These hardships force security teams to operate in a reactive rather than proactive mode, so the organization is at greater risk of experiencing incidents and being unable to detect and respond to them promptly. Moreover, even though businesses are relying on IT much more in the wake of the pandemic and stay-at-home orders, most IT teams didn't have their security budget increased. As a result, they need to juggle ever-limited resources to pull the company through a more sophisticated threat landscape, so we will keep living in the "new day, new breach" reality. To overcome the challenge of limited resources, we advise organizations to outsource IT tasks to MSSPs or/and invest in tools that automate routine IT tasks.

Beware of supply chain attacks.

Incidents that included supply chain compromise had the most impact on organizations; they were more likely to result in compliance fines, decrease in new sales, change in senior leadership and even lawsuits than any other incident types. To avoid these consequences, organization need to pay attention to the less-secure elements in their supply network. Proven security best practices to mitigate these risks include network segmentation, continuous auditing for malicious activity across the environment and alerting to suspicious actions. Organizations should ask partners to prove that they take all necessary security measures, such as third-party audits or confirmation of usage of certain security services and/or tools. Organizations can also limit their liability under their contracts with partners and make them accountable in the event that they experience a data breach.

Think business when assessing security risks.

To drive adaptive security and ensure adequate attention to real risks, IT professionals should identify threat/vulnerability pairs and determine the consequences they pose to organization. Our research showed that it is of critical importance to look beyond classic consequences, such as unplanned expenses or compliance fines. Certain types of threats (e.g., supply chain compromise and data theft) can have far more severe outcomes that affect the company's financial well-being, such as a negative impact on valuation or churn rates. Therefore, when assessing security risks. security leaders are advised to include the long-term consequences of data breaches on the business as a whole.

APPENDIX 1:

VERTICALS

FINANCE

53% of financial organizations store customer data in the cloud, and 35% store financial data there.

Top 3 data security incidents in the cloud

Phishing attacks	26%
Targeted attacks on cloud infrastructure	22%
Ransomware or other malware attacks	15%

Top 3 data breach outcomes

Unplanned expenses to fix security gaps	20%
Compliance fines	19%
Customer churn	17%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Targeted attacks on cloud infrastructure	17%	42%	21%	20%	0%	0%
Phishing attacks	58%	26%	16%	0%	0%	0%
Ransomware or other malware attacks	23%	49%	28%	0%	0%	0%

89% of financial organizations needed months to discover insider data theft.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Targeted attacks on cloud infrastructure	28%	34%	21%	17%	0%	0%
Phishing attacks	41%	45%	14%	0%	0%	0%
Ransomware or other malware attacks	27%	46%	26%	0%	0%	0%

52% of financial organizations needed weeks to recover from supply chain compromise.

Top 3 cybersecurity challenges

59%	Understaffed IT/security
44%	Lack of expertise in cloud security
37%	Employee negligence

Top 3 security measures

	Already do	Plan to do	Don't plan to do
Employee training	77%	23%	0%
Auditing of user activity	70%	22%	7%
Review of access rights (attestation)	65%	35%	0%

37% of financial organizations plan to start classifying data, and 40% plan to implement multifactor authentication (MFA).

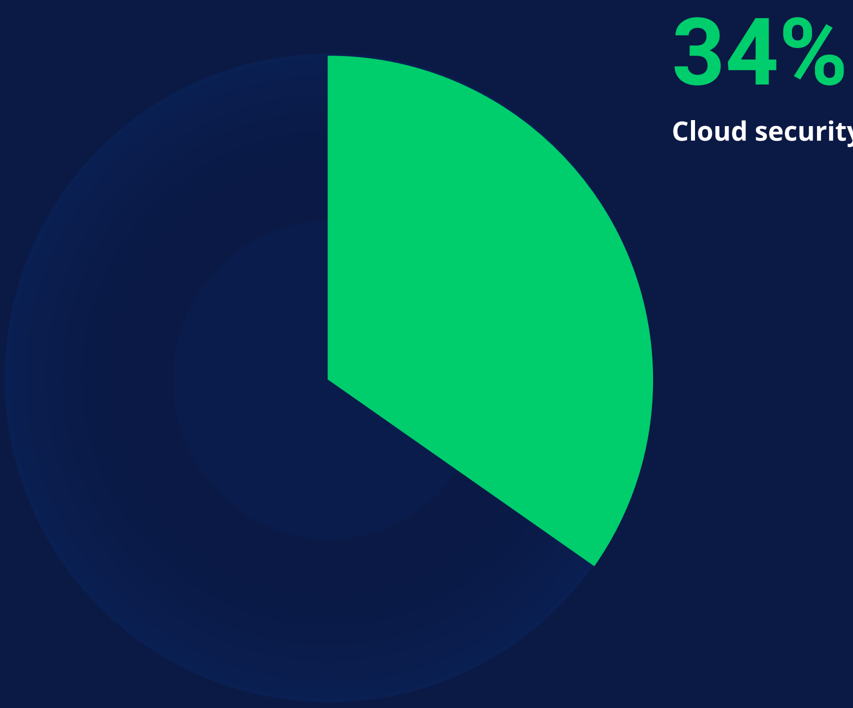
Impact of the pandemic on cybersecurity spending

33%
Cybersecurity spending increased

30%
Spending stayed the same, but priorities changed

19%
Spending decreased

Cybersecurity budget distribution



EDUCATION

48% of educational organizations store employee data in the cloud, while 30% store student data.

Top 3 data security incidents in the cloud

Phishing attacks	60%
Account compromise	33%
Ransomware or other malware attacks	27%

Top 3 data breach outcomes

Unplanned expenses to fix security gaps	33%
Customer churn	10%
Decrease in company valuation	9%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	44%	33%	23%	0%	0%	0%
Account compromise	18%	54%	28%	0%	0%	0%
Ransomware or other malware attacks	32%	19%	49%	0%	0%	0%

93% of educational organizations needed days or weeks to discover accidental data leakage.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	29%	35%	36%	0%	0%	0%
Account compromise	34%	18%	48%	0%	0%	0%
Ransomware or other malware attacks	21%	46%	33%	0%	0%	0%

33% of educational organizations needed weeks to recover from accidental data leakage.

Top 3 cybersecurity challenges

53%	Understaffed IT/security
52%	Lack of expertise in cloud security
49%	Lack of budget

Top 3 security measures

	Already do	Plan to do	Don't plan to do
Cloud backups	54%	25%	21%
Auditing of user activity	53%	20%	27%
Review of access rights (attestation)	53%	27%	20%

40% of educational organizations plan to deploy data classification, and 36% will deploy MFA.

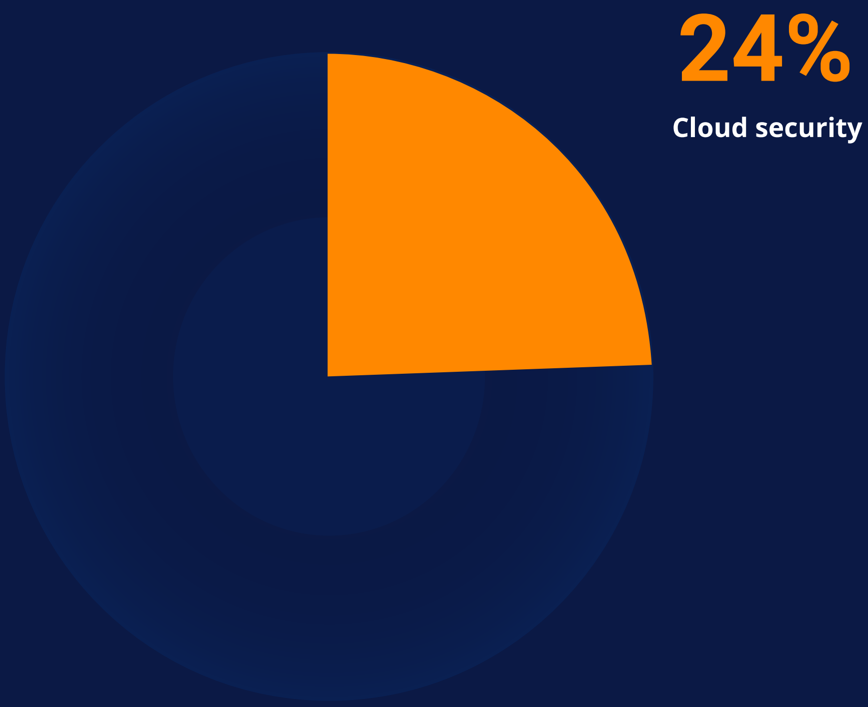
Impact of the pandemic on cybersecurity spending

20%
Cybersecurity spending increased

33%
Spending and priorities stayed the same

27%
Spending stayed the same, but priorities changed

Cybersecurity budget distribution



GOVERNMENT

50% of government agencies do not store any data in the cloud. 29% store employee data and 25% store financial information.

Top 3 data security incidents in the cloud

Phishing attacks	39%
Accidental data leakage	24%
Targeted attacks on cloud infrastructure	22%

Top 3 data breach outcomes

Unplanned expenses to fix security gaps	28%
Customer churn	13%
Change in senior leadership	11%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	33%	67%	0%	0%	0%	0%
Accidental data leakage	31%	42%	27%	0%	0%	0%
Targeted attacks on cloud infrastructure	12%	86%	2%	0%	0%	0%

34% of government agencies spent weeks to discover data loss.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	29%	67%	4%	0%	0%	0%
Accidental data leakage	9%	25%	32%	11%	23%	0%
Targeted attacks on cloud infrastructure	8%	47%	12%	14%	19%	0%

67% of government agencies needed months to recover from account compromise and data loss.

Top 3 cybersecurity challenges

65%	Understaffed IT/security
59%	Employee negligence
53%	Lack of budget

Top 3 security measures

	Already do	Plan to do	Don't plan to do
Auditing of user activity	65%	24%	12%
Data classification	56%	19%	25%
Review of access rights (attestation)	53%	29%	18%

41% of government agencies plan to implement employee training, and the same percentage plan to implement encryption.

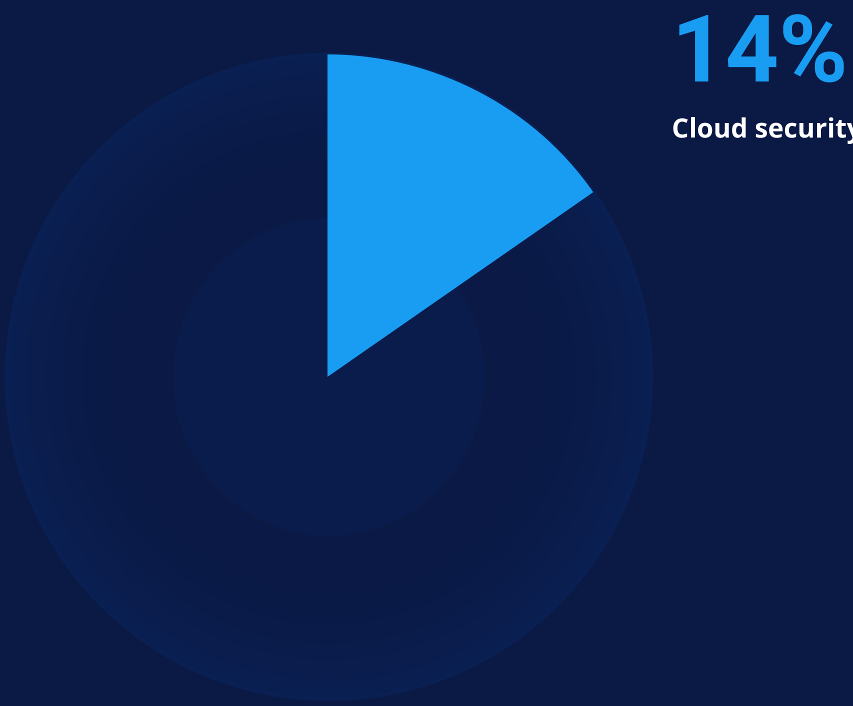
Impact of the pandemic on cybersecurity spending

24%
Cybersecurity spending increased

24%
Spending and priorities stayed the same

47%
Spending stayed the same, but priorities changed

Cybersecurity budget distribution



HEALTHCARE

61% of healthcare organizations store customer data in the cloud, and 54% store personal healthcare records there.

Top 3 data security incidents in the cloud

Phishing attacks	44%
Ransomware or other malware	39%
Data theft by insiders	35%

Top 3 data breach outcomes

Unplanned expenses to fix security gaps	24%
Compliance fines	23%
Lawsuits	11%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	49%	38%	13%	0%	0%	0%
Ransomware or other malware attacks	42%	43%	15%	0%	0%	0%
Data theft by insiders	16%	32%	24%	28%	0%	0%

32% of healthcare organizations needed days to discover accidental data leakage and supply chain compromise.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	37%	38%	25%	0%	0%	0%
Ransomware or other malware attacks	5%	67%	28%	0%	0%	0%
Data theft by insiders	4%	53%	43%	0%	0%	0%

22% of healthcare organizations needed weeks to recover from targeted attacks on cloud infrastructure.

Top 3 cybersecurity challenges

61%	Lack of budget
56%	IT/security team being understaffed
39%	Employee negligence

Top 3 security measures

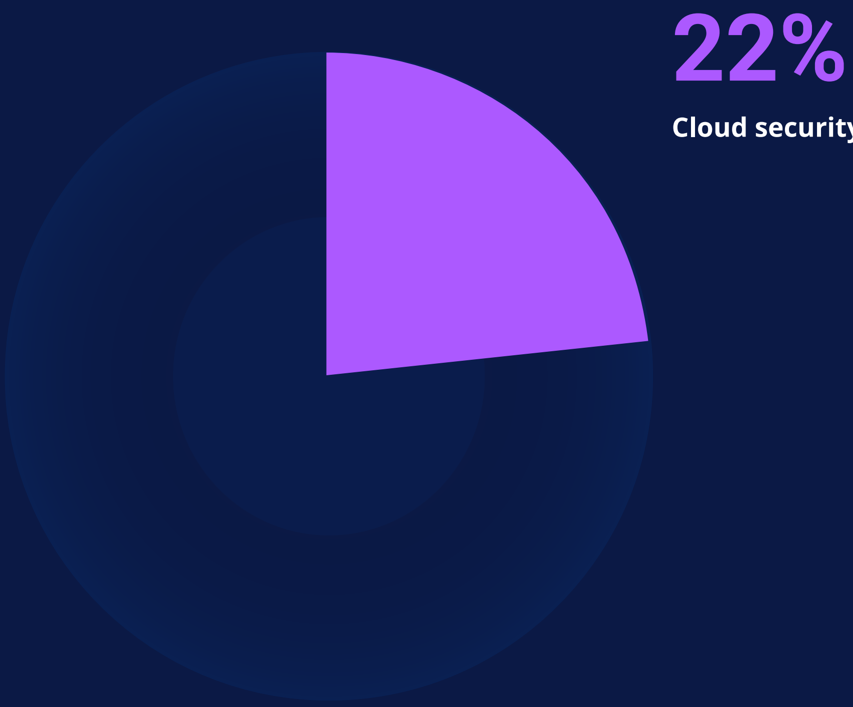
	Already do	Plan to do	Don't plan to do
Encryption	78%	17%	6%
Review of access rights (attestation)	75%	13%	13%
Employee training	65%	29%	6%

35% of healthcare organizations plan to implement MFA, while 31% will start auditing user activity.

Impact of the pandemic on cybersecurity spending

22% Cybersecurity spending increased	**39%** Spending and priorities stayed the same	**22%** Spending decreased

Cybersecurity budget distribution



APPENDIX 2:

GEOGRAPHY

NORTH AMERICA

46% of U.S. organizations store customer data in the cloud.

Top 3 data security incidents in the cloud

Phishing attacks	50%
Ransomware or other malware attacks	27%
Accidental data leakage	19%

Top 3 data breach outcomes

Unplanned expenses to fix security gaps	32%
Loss of competitive edge	12%
Decrease in company valuation	10%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	42%	44%	15%	0%	0%	0%
Ransomware or other malware attacks	47%	43%	7%	3%	0%	0%
Accidental data leakage	11%	37%	42%	11%	0%	0%

25% of U.S. organizations needed weeks to discover insider data theft, and 13% required months to detect supply chain compromise.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	36%	42%	18%	4%	0%	0%
Ransomware or other malware attacks	20%	47%	20%	10%	3%	0%
Accidental data leakage	5%	53%	21%	16%	5%	0%

20% of U.S. organizations needed months to recover from data theft caused by hackers.

Top 3 cybersecurity challenges

53%	Lack of budget
50%	IT/security team being understaffed
44%	Lack of expertise in cloud security

Top 3 security measures

	Already do	Plan to do	Don't plan to do
Employee training	69%	22%	8%
Encryption	69%	25%	6%
Auditing of user activity	65%	28%	8%

32% of U.S. organizations plan to start attestation of user privileges, while 30% plan to deploy data classification.

Impact of the pandemic on cybersecurity spending

30%
Cybersecurity spending increased

30%
Spending stayed the same, but priorities changed

23%
Spending and priorities stayed the same

On average, U.S. organizations allocate **27%** of their cybersecurity budget to cloud security.

UNITED KINGDOM

42% of UK organizations store customer data in the cloud.

Top 3 data security incidents in the cloud

Phishing attacks	52%
Ransomware or other malware attacks	23%
Account compromise	21%

Top 3 data breach outcomes

Unplanned expenses to fix security gaps	36%
Customer churn	14%
Decrease in new sales	12%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	54%	32%	14%	0%	0%	0%
Ransomware or other malware attacks	27%	26%	47%	0%	0%	0%
Account compromise	7%	42%	46%	5%	0%	0%

28% of UK organizations needed weeks to discover insider data theft, and 15% spent months to detect supply chain compromise.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	14%	64%	22%	0%	0%	0%
Ransomware or other malware attacks	4%	13%	83%	0%	0%	0%
Account compromise	24%	23%	53%	0%	0%	0%

29% of UK organizations needed months to recover from data theft caused by hackers.

Top 3 cybersecurity challenges

63%	IT/security team being understaffed
51%	Lack of budget
50%	Inconsistent tools and processes due to multiple workloads across different cloud platforms

Top 3 security measures

	Already do	Plan to do	Don't plan to do
Employee training	86%	4%	10%
Encryption	74%	12%	14%
Cloud backups	65%	15%	20%

50% of UK organizations plan to start auditing user activity, while 44% plan to implement regular review of access rights.

Impact of the pandemic on cybersecurity spending

22%
Cybersecurity spending increased

54%
Spending stayed the same, but priorities changed

11%
Spending decreased

On average, UK organizations allocate **25%** of their cybersecurity budget to cloud security.

FRANCE

47% of French organizations store customer data in the cloud.

Top 3 data security incidents in the cloud

Phishing attacks	38%
Data loss	31%
Targeted attacks on cloud infrastructure	23%

Top 3 data breach outcomes

Customer churn	17%
Compliance fines	11%
Loss of competitive edge	8%

Time to detect most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	76%	17%	7%	0%	0%	0%
Data loss	48%	25%	27%	0%	0%	0%
Targeted attacks on cloud infrastructure	33%	62%	5%	0%	0%	0%

35% of French organizations needed weeks to discover account compromise.

Time to resolve most common security incidents in the cloud

	MINUTES	HOURS	DAYS	WEEKS	MONTHS	YEARS
Phishing attacks	54%	32%	14%	0%	0%	0%
Data loss	11%	85%	4%	0%	0%	0%
Targeted attacks on cloud infrastructure	24%	58%	18%	0%	0%	0%

52% of French organizations needed weeks to recover from accidental data leakage.

Top 3 cybersecurity challenges

75%	Employee negligence
56%	IT/security team being understaffed
54%	Lack of visibility into sensitive data in the cloud

Top 3 security measures

	Already do	Plan to do	Don't plan to do
Auditing of user activity	54%	23%	23%
Encryption	51%	32%	17%
Review of access rights (attestation)	50%	36%	14%

58% of French organizations plan to implement MFA, while 42% plan to deploy data classification.

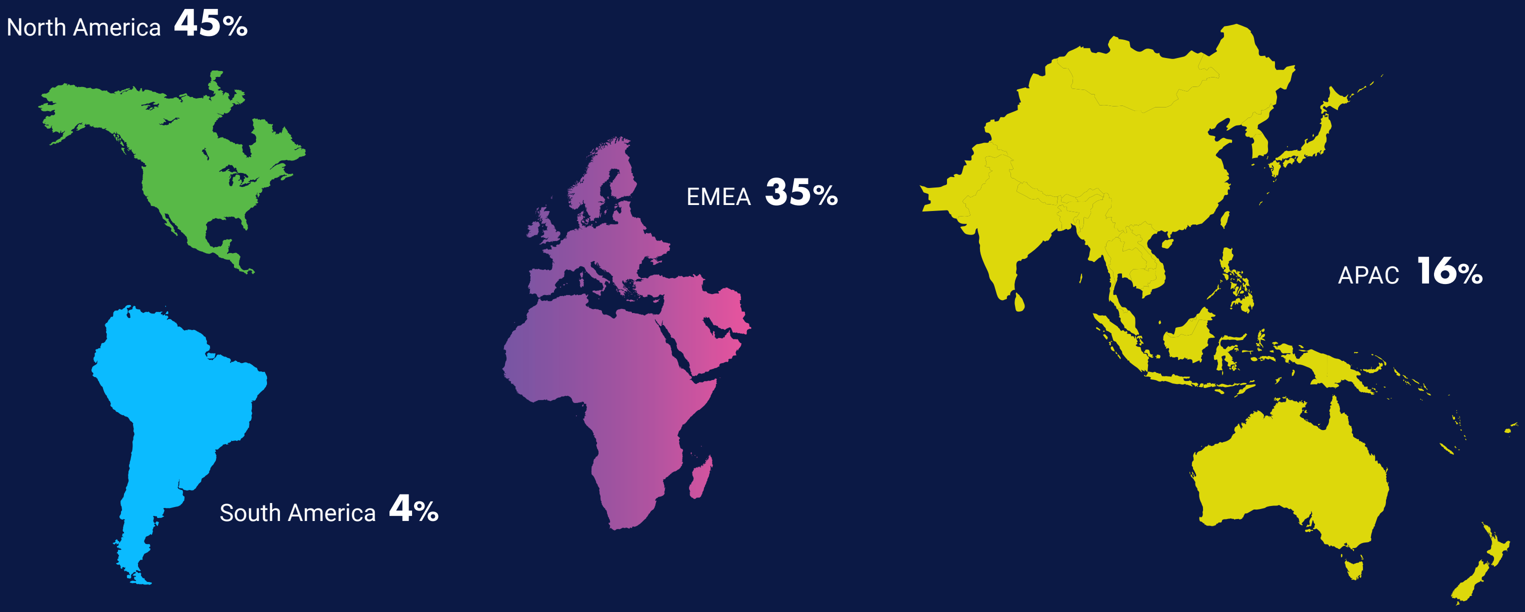
Impact of the pandemic on cybersecurity spending

27% Spending increased	**55%** Spending stayed the same but priorities changed	**9%** Spending decreased

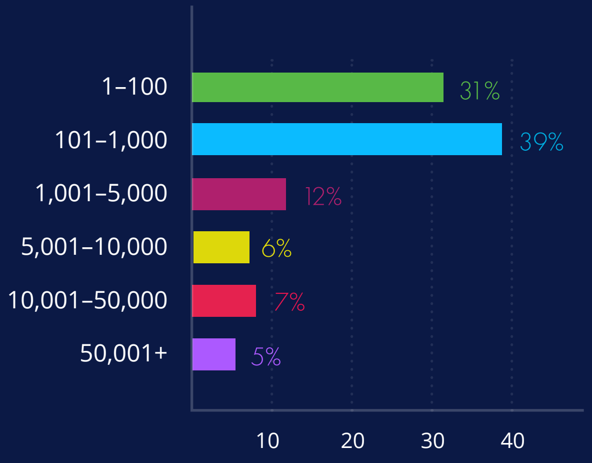
On average, French organizations allocate **36%** of their cybersecurity budget to cloud security.

APPENDIX 3:

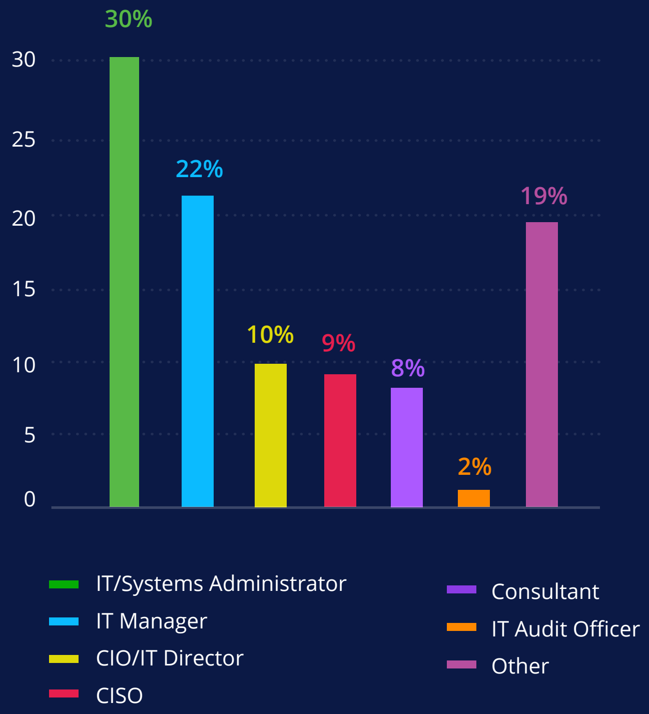
SURVEY DEMOGRAPHICS



ORGANIZATION SIZE (Employees)



TOP JOB TITLES



TOP INDUSTRIES

Technology/managed services	11%
Manufacturing	10%
Technology/software	10%
Banking & finance	9%
Education	7%
Healthcare	6%
Consulting	6%
Government	6%
Services	5%
Retail & Wholesale	4%
Insurance	3%
Energy	3%
Technology/hardware	3%
Telecommunications	3%
Entertainment & leisure	3%

ABOUT THE REPORT

The report is brought to you by Netwrix Research Lab, which conducts industry surveys among IT pros worldwide to discover important changes and trends. For more reports, please visit www.netwrix.com/go/research

ABOUT NETWRIX

Netwrix makes data security easy by simplifying how professionals control sensitive, regulated and business-critical data, regardless of where it resides. More than 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