Acronis

Report 2022

Acronis Cyber Protection Week Global Report

Acronis

Cyber Protection Week Global Report 2022

Table of contents

Introduction & Survey methodology

Crippling cyberattacks, data exfiltration and data breaches have become parts of our everyday lives. Never before have organizations and individuals been so inundated with news and guidance on the very real — and very damaging — cyberthreats threatening personal and professional IT users around the world.

However, while awareness of these threats continues to grow, we're seeing a massive gap in how organizations and individuals approach cyber protection, both in theory and in practice.

To explore the extent of that gap and the reasons behind it, Acronis commissioned an independent survey of over 6,200 IT users and IT managers, from small businesses to enterprises, across 22 countries. The findings expose some of the most critical shortcomings appearing in cyber protection practices today, examine why they're appearing and offer guidance on how they can be fixed.

This report explores:

- How well organizations and individuals adopt essential cyber protection practices
- Gaps between the perceived and actual cyber readiness of IT teams
- How prepared IT teams are for cyberthreats in 2022

To explore the extent of that gap and the reasons behind it, Acronis commissioned an independent survey of over 6,200 IT users and IT managers, from small business to enterprises, across 22 countries. The findings expose some of the most critical shortcomings appearing in cyber protection practices today, examine why they're appearing and offer guidance on how they can be fixed.

About the survey methodology

Acronis surveyed 6,200 IT managers and IT users to examine their approach and experiences with today's cyber protection solutions and cyberthreats landscape. Acronis had no role in selecting the respondents. All responses were anonymous. The survey was conducted in March 2022.

Within each country, 50% of respondents were IT managers at organizations ranging in size from SMB to enterprise in both public and private sectors. The other 50% were independent IT users.

Respondents came from 22 countries across six continents:

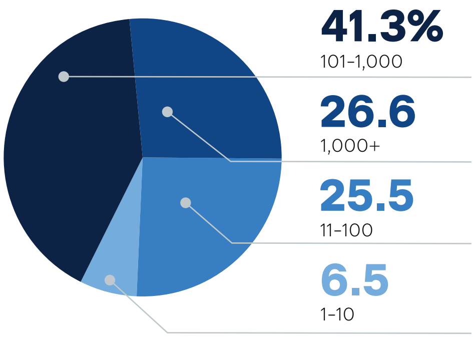
Country	Respondents
Australia	257
Brazil	722
Bulgaria	200
Canada	256
China	389
Denmark	201
France	221
Germany	223
India	386
Italy	207
Japan	233
Netherlands	200
Saudi Arabia	407
Singapore	232
South Africa	249
South Korea	344
Spain	200
Sweden	178
Switzerland	200
United Arab Emirates	200
United Kingdom	294
USA	437

Key industries represented:

- IT/Telecom
- Finance
- Healthcare
- Education

Organizations represented by IT managers – number of employees:

How many employees does your organization have?



Executive summary

Key research findings

IT users

Despite growing awareness and increasing threats, people's backup habits remain unchanged

- Only 10% of users back up daily, 15% of users back up once or twice a week — while 34% of users back up on a monthly basis. 41% of users rarely or never back up their data.
- Still, 72% of all users had to recover from backup at least once in the past year (33% — more than once). Meaning some of the users who choose not to back up have permanently lost data.
- Only 12% of IT users are using the best practice hybrid model of cloud and local backup storage — the same response as last year.
- Users double down on cloud backup: for four years, local backups have been shrinking — from 62% in 2019 to 33% in 2022, almost a two-fold decrease. All while cloud backups grew from 28% in 2019 to 54% in 2022. Still, only 12% of users use the hybrid local and cloud strategy.

Knowing is not enough: users show concern over cyberthreats, but not action

- Over half of all personal IT users (56%) lost data at least once in 2021 — 26% lost it multiple times.
- 66% of users would not know or be able to tell if their data was modified.
- 43% of personal IT users are not sure if their anti-malware solutions could protect against new and emerging cyberthreats. Another 16% are confident that they couldn't.
- Too little, too late: 43% of users update a week or more after an update release — a steady decline in response time across the board compared to 2021. Of those, 7% take more than a month to perform these recommended updates.
- 71% of IT users are worried about geopolitical cyberattacks, but their concern does not translate into improvements to their cyber protection.

Cybercriminals are hiding behind complexity

- The top five cyberthreats that users are most concerned with: Data theft (credit card, identity, passwords, etc.); Malware (virus, etc.); Phishing attacks; Brute forcing (having a weak password); Ransomware.
- Users still don't know much about some of the major cyberthreats they're facing — counting on this lack of awareness, cybercriminals use elaborate and sophisticated attack vectors that people don't think about.
- Even highly publicized, and effective, cyberattack vectors like cryptojacking and DoS/DDoS are discounted by a significant percentage of personal IT users — 43% aren't concerned or aware of cryptojacking, 36% aren't concerned or aware of DoS/DDoS attacks.

Tip: Phishing attacks and ransomware remain the most common and effective forms of cyberattack. Learn how to detect and overcome them with the Acronis Cyberthreats Report 2022.

IT managers

"More solutions" doesn't mean "more protection"

- 61% of organizations have between 6 and 15 different protection and security tools running simultaneously. 22% of companies are using more than 10 different tools.
- Despite this, 76% of organizations experienced downtime due to data loss in the last year. That's a 25% increase from our 2021 results. This downtime stemmed from a number of sources including system crashes (52%), human error (42%), cyberattacks (36%) and insider attacks (20%).
- As a result, 61% of IT professionals report a preference for integrated solutions that replace their complicated stacks of cybersecurity and data protection tools with a single, unified console.

A lack of awareness is creating a lack of protection

- Pandemic-fueled frequent backups are over: a third of IT managers back up weekly, another 25% monthly. Use of backup best practices is declining — only 15% of IT managers adhere to them.
- Reality check: 20% of IT managers claim to be testing backup restoration weekly.
- 76% of companies have suffered downtime in the past year — system crashes, human error and cyberattacks are among the top causes. This represents a 25% increase over our 2021 report.
- Same as last year, 10% of IT managers still aren't sure if their company is subject to any data privacy regulations. This goes to prove that IT managers, like IT users, get stuck in their ways.

Overconfidence as a trend — overselling IT teams' readiness

- 70% of IT managers claim to have automated patch management — however, based on our observations, only a handful of companies follow the 72-hour "golden time" for patch management.
- 82% of respondents claim to have ransomware protection and remediation — yet, successful attacks occur weekly and the size of ransom demands grows each year.
- 86% of IT managers are concerned about the threat of increasing politically-driven cyberattacks.
- Half of organizations allocate less than 10% of their IT budget on IT security.
- Only 23% of companies are investing over 15% of their overall IT budget into security — despite the increasingly threatening cyber landscape.

Part 1

IT users

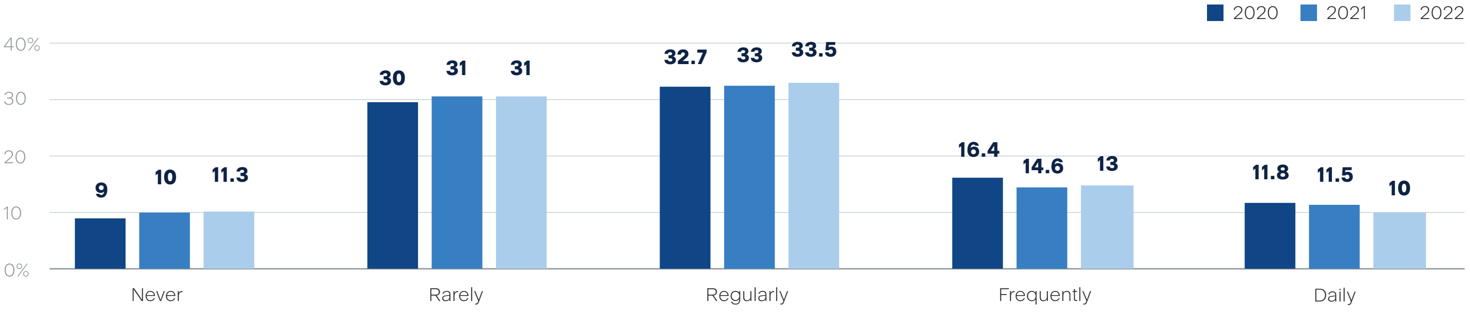
To investigate the changes in global cyberthreat landscape, Acronis commissioned an independent survey featuring over 2,669 IT users across 22 countries. Keep reading for the key findings.

Only one in ten users backs up daily

#1

How often do you back up your computer and mobile devices?

Backup habits are hard to alter. Consistent with last year's Cyber Protection Week Report, 10% of individual users never back up. 52% of them believe it's unnecessary, 28% of them say it's too complicated and the rest believe it takes too long or is too expensive.



IT users doubling down on cloud backup storage

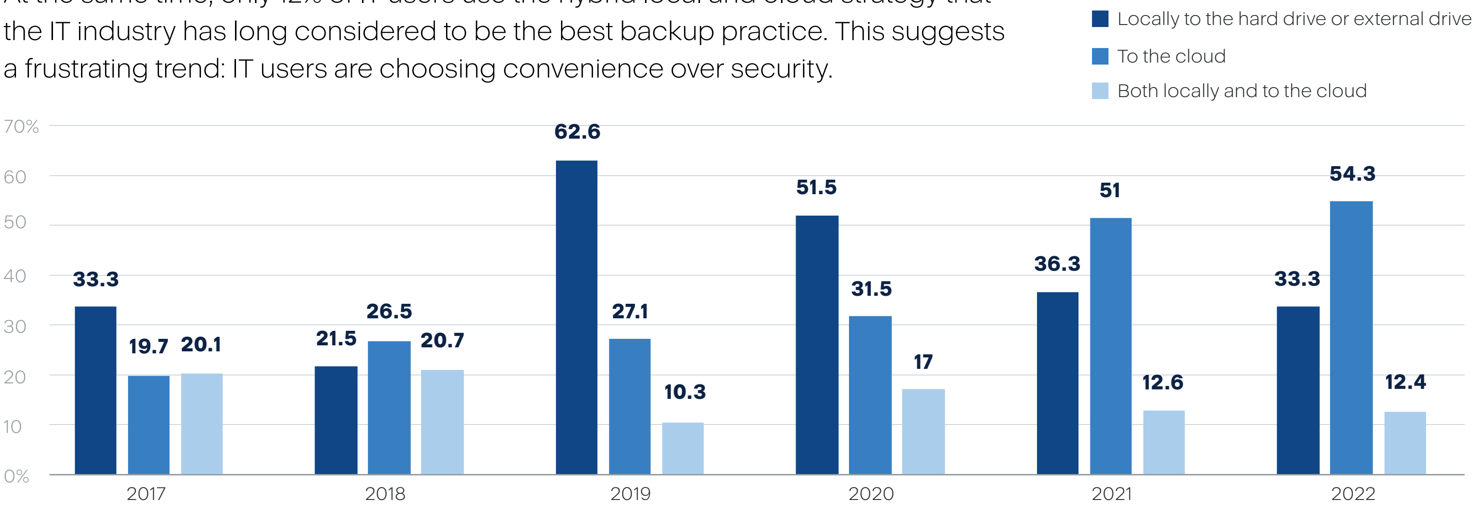
#2

When you do back up, where do you back up to?

For four years in a row, we've seen the use of local backups shrinking — from 62% in 2019 to 33% in 2022. That's almost a two-fold decrease. At the same time, cloud backups have doubled in popularity from 27% in 2019 to 54% in 2022. Clearly, users have learned to trust the cloud and now use it more frequently.

Part of this growth is likely because public cloud solutions perform backups automatically, an example of broader automatic protection features that individuals and organizations are depending on more and more.

At the same time, only 12% of IT users use the hybrid local and cloud strategy that the IT industry has long considered to be the best backup practice. This suggests a frustrating trend: IT users are choosing convenience over security.

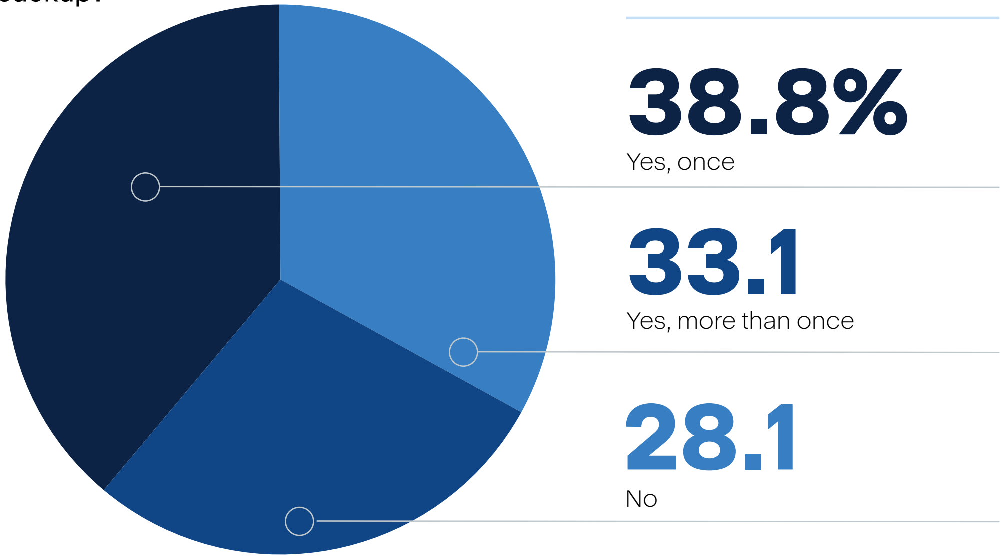


IT users are relying on their backups, though they're far from optimized

#3

Have you ever had to recover from a backup?

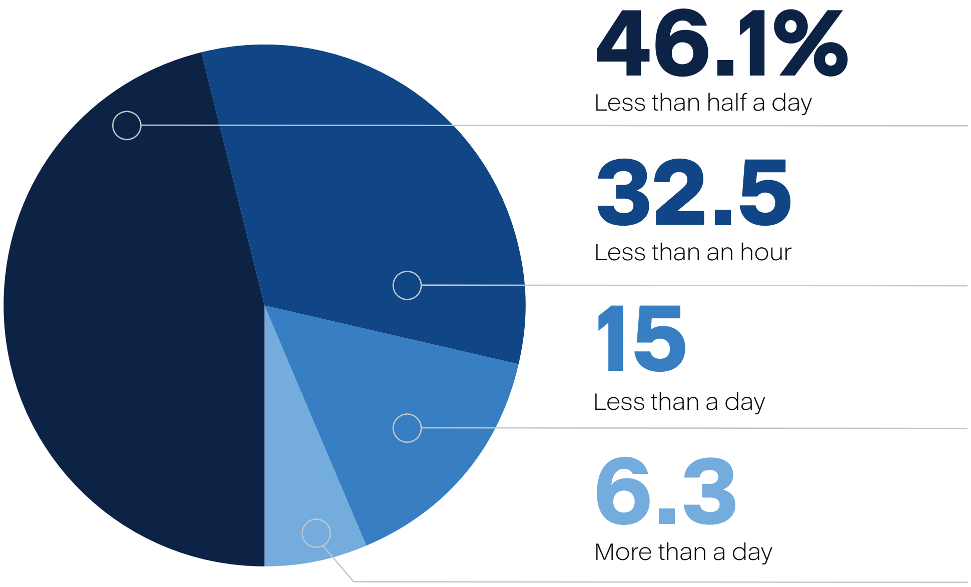
Interestingly, while 41% of all IT users either rarely or never back up their data, 72% of all users have had to rely on backups to recover lost data in the past (33% of them more than once). Meaning, the lack of a reliable backup caused some IT users to lose their data permanently.



#4

How long did it take for you to restore your system from a backup?

When performing recoveries from backups less than one-third of IT users were able to regain their data in less than an hour. For 46% of respondents, recoveries could take up to 12 hours. Longer recovery times may stem from unfamiliarity with the technology or issues with the way the backup was performed.

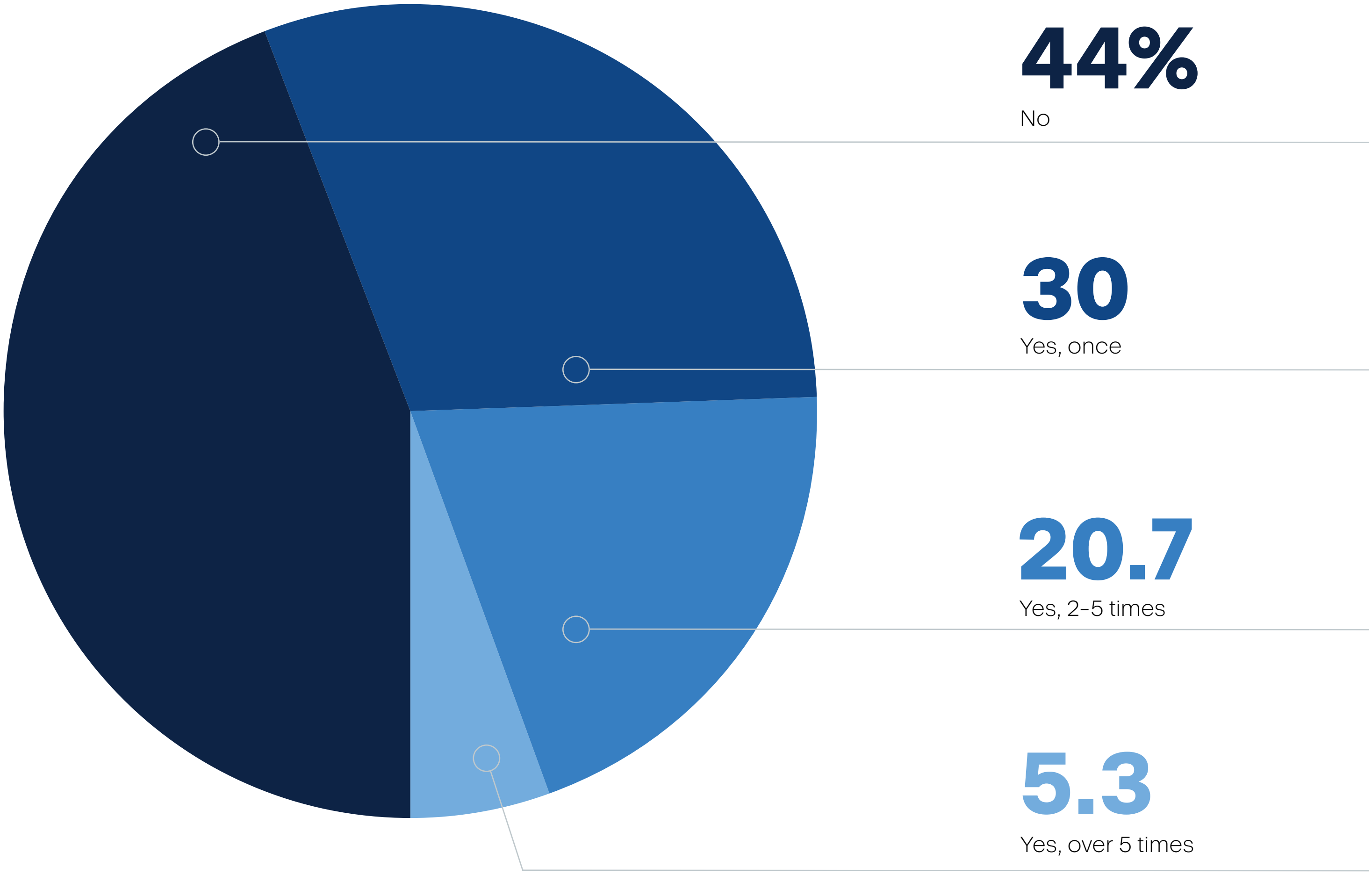


Over half of personal IT users permanently lost data in 2021

#5

In the last year, have you or a family member permanently lost data from a computer or mobile device?

56% of IT users lost data at least once in the past year due to accidental deletions, app/system crashes, malware attacks, lost/stolen device, and others. 26% lost data multiple times. We believe the increasing number of connected devices and the growing complexity involved in protecting them to be the main causes for this common shared experience.



Cybercriminals are hiding behind complexity

Cyberthreats IT users are most concerned with:

65%	Data theft (credit card, identity, passwords, etc.)
59%	Malware (virus, etc.) attacks
49%	Phishing attacks
47%	Brute forcing (having a weak password)
42%	Ransomware

Cyberthreats IT users aren't familiar with:

26%	Cryptojacking
20%	Denial of service (DoS or DDoS) attacks
19%	Home automation, Internet of Things (IoT) attacks

Despite cyberattacks appearing regularly in the news, people still don't know much about major cyberthreats they're facing. That's creating a window of opportunity for cybercriminals. Counting on this lack of awareness, cybercriminals are using elaborate and sophisticated attack vectors that people don't think about.

The shocking lack of awareness of certain attack vectors likely stems from the false belief that elaborate cyberattacks aren't targeting individual users — a belief that has been proven incorrect countless times.

Among the attack vectors IT users are familiar with, brute forcing weak passwords has maintained a position at the top of mind since the 2020 shift to remote work, when the importance of strong passwords became obvious to many.

Tip:

Enable multi-factor authentication in addition to strong passwords to reduce your risk of falling victim to many common and dangerous cyberthreats.

Precautions taken during the pandemic prove temporary

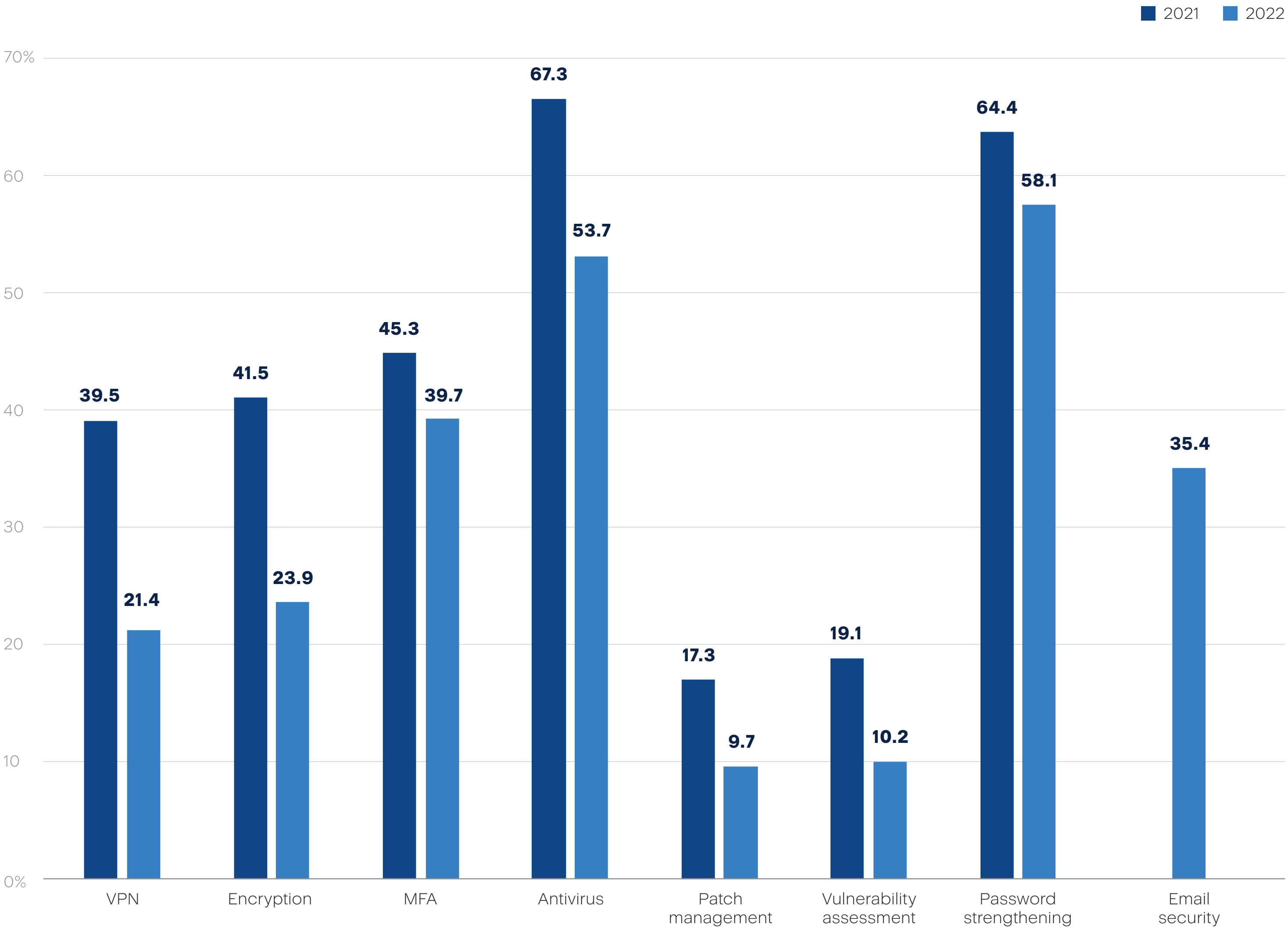
#6

What extra precautionary steps did you take this year?

There is a significant gap between the reliance IT users place on their data and devices and how much they're doing to protect them. Across the board, IT users are reporting fewer precautionary measures compared to last year.

While the pandemic may have caused people to take extra steps to defend their data, devices and privacy, users in 2022 are becoming complacent. They aren't being as active in their use of these defenses, creating opportunities for cybercriminals.

Similar to last year's Cyber Protection Week report results, patch management, vulnerability assessment, VPN and encryption prove to be the least adopted.

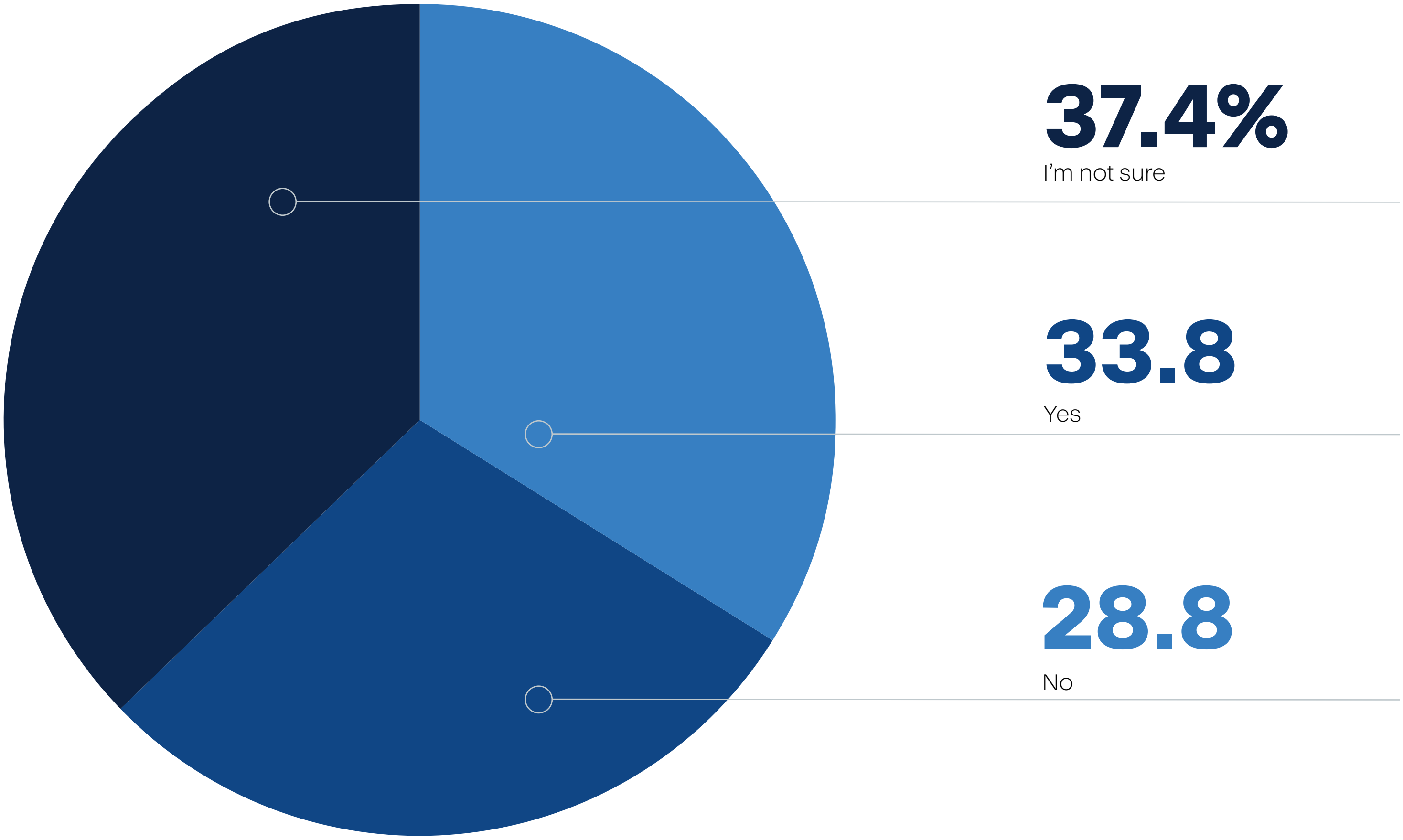


66% of users would not know or be able to tell if their data was modified

#7

Would you know if any of your data had been unexpectedly accessed or modified?

66% of IT users wouldn't know for sure if their data was accessed or modified — either because they lack tools that offer these alerts, or because they don't know how to use their tools to find out. In either case, this represents a shocking blindspot in the safety and security of peoples' data. What's worse, based on Acronis previous findings and observations, we believe that number should be much higher.

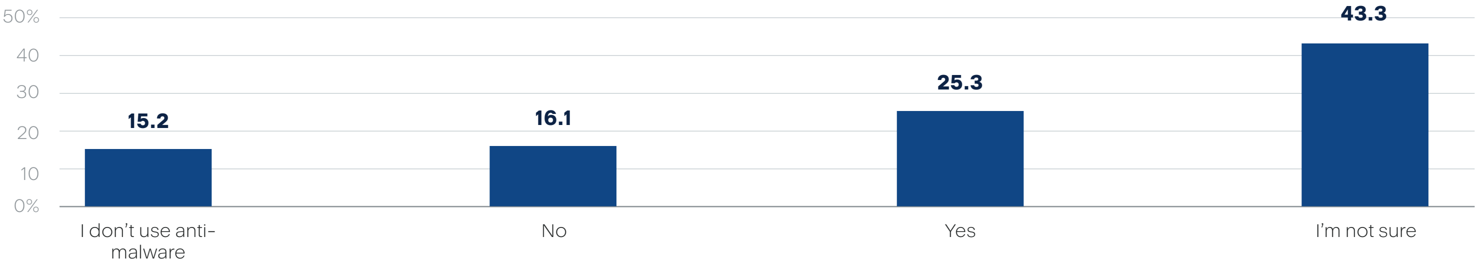


More than half of personal IT users can't stop zero-day threats (or aren't sure)

#8

Does your anti-malware protect against never-before-seen (zero-day) cyberthreats?

43% of personal IT users are not sure if their anti-malware solutions could protect against new and emerging cyberthreats. Another 16% are confident that they couldn't. This poses a serious threat — a lack of knowledge is certain to lead to a lack of security.



Too little, too late: 43% of users update a week or more after an update release

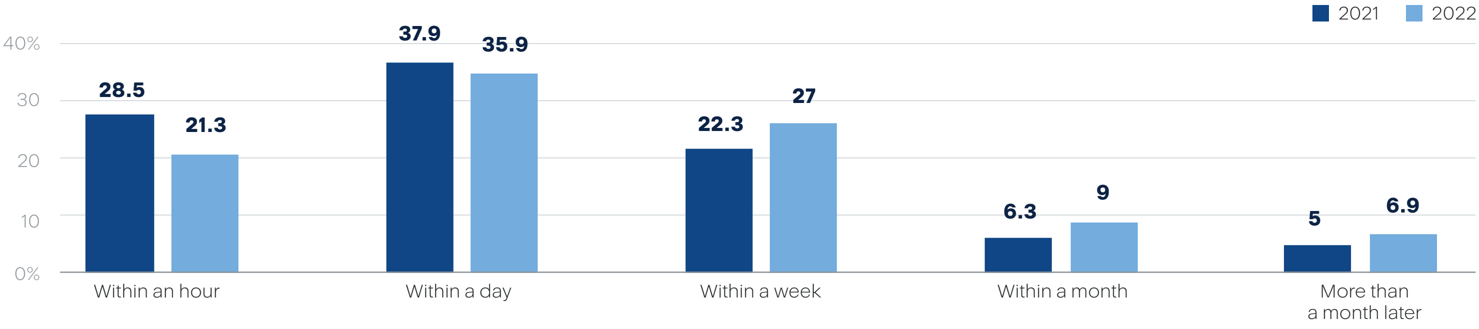
#9

On average, how soon after getting notified that your device needs an update do you update/restart?

Personal IT users demonstrate a steady decline in response time across the board compared to 2021. 43% of users now take a week or more to update their software after they're notified that one is available, leaving a huge window for vulnerabilities to be exploited by cybercriminals. Of those, 7% take more than a month to perform these recommended updates, which means that in some cases (including Microsoft updates) there will already be new patches available before they apply the old ones.

Case in point: The US Department of Defense first identified their vulnerability to the log4j exploit. Reported on Dec. 17, and fixed the vulnerability on Dec. 31.

Tip: The "Golden time" for patch management is 72 hours. As proven in the latest case of log4j and Windows vulnerabilities. Vulnerabilities that are easier to exploit demand an even faster response time.



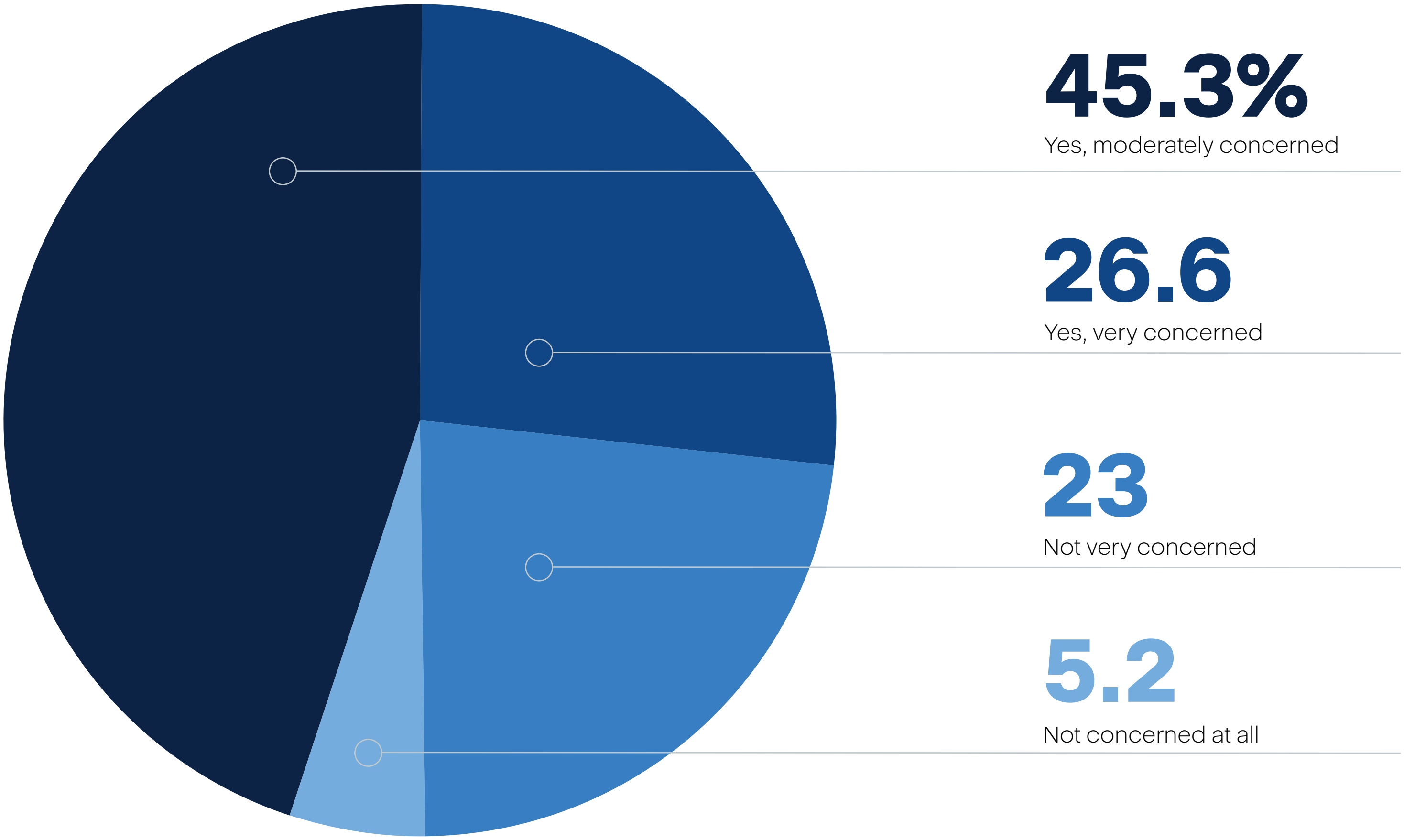
Concerned, but idle: 71% of IT users are worried about geopolitical cyberattacks

#10

Are you concerned about increased cyberattacks caused by the current geopolitical climate?

To clarify, it's not state-sponsored attacks that would be the primary cause of concern for IT users. Instead, they should worry about politically-driven hacking groups leveraging any geopolitical conflict and causing accidental — or intentional — damage.

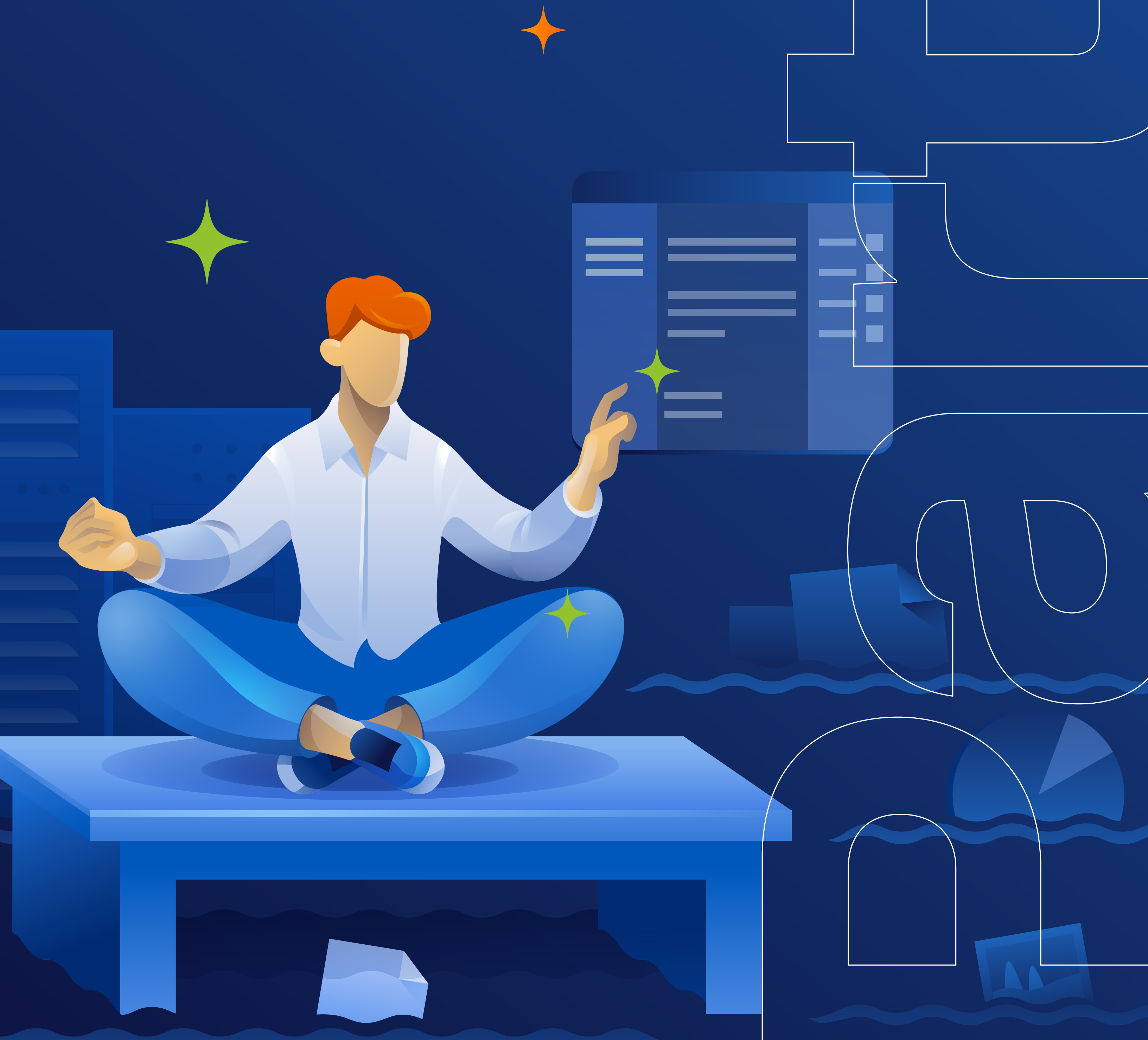
Surveyed in March 2022, 28% of IT users claim they aren't particularly concerned about this threat. However, over two-thirds (71%) of IT users are moderately or very concerned about these attacks increasing. Based on the full findings of this report, IT users may be more alert, but their concern may not translate into improvements to their cyber protection.



Part 2

IT managers

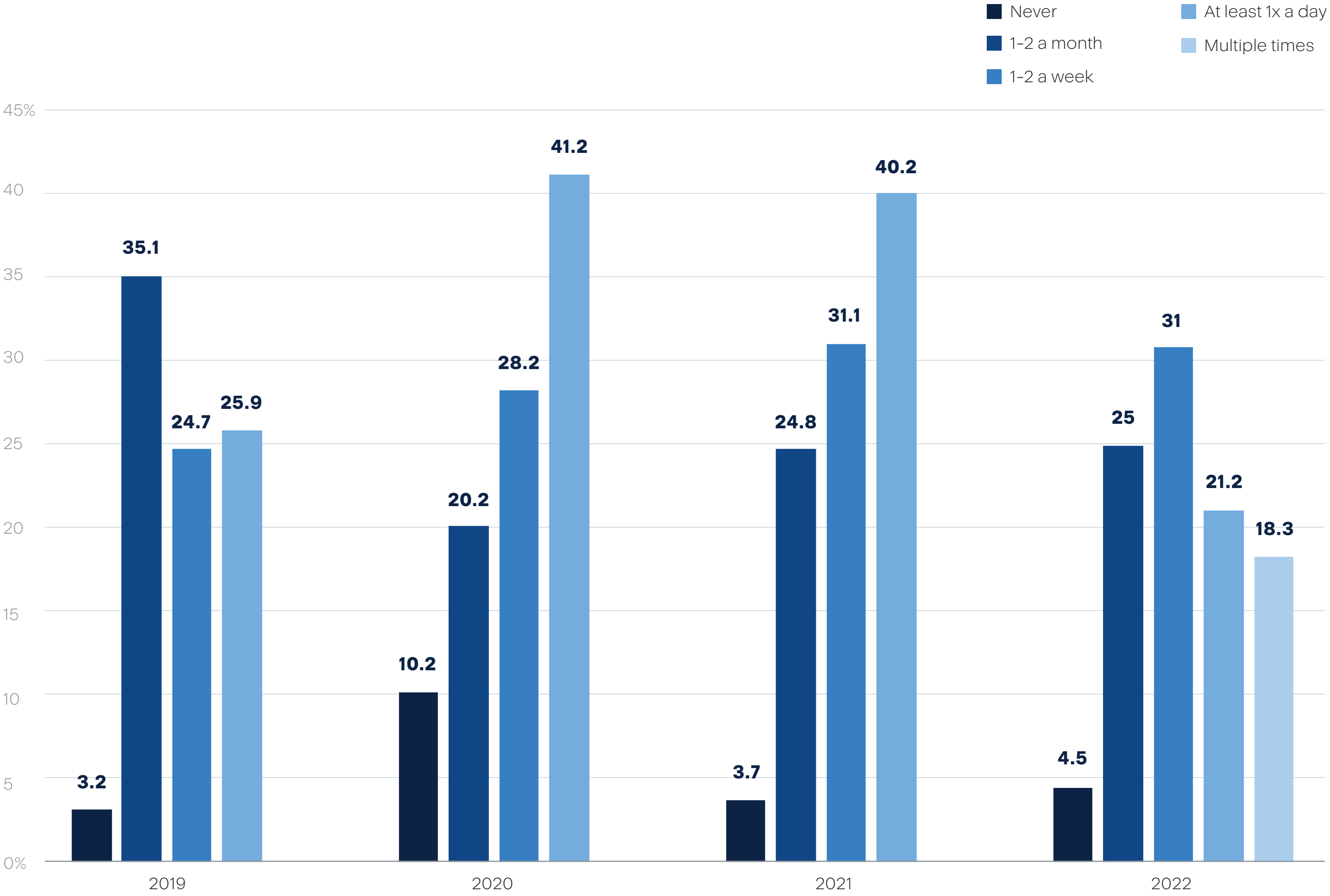
To investigate the changes in global cyberthreat landscape, Acronis commissioned an independent survey featuring over 3,567 IT managers, from small business to enterprises, across 22 countries. Keep reading for the key findings.



Pandemic-fueled frequent backups are over: a third of IT managers back up weekly, 25% just monthly

#1

How often do you back up the IT environment components your organization is responsible for?



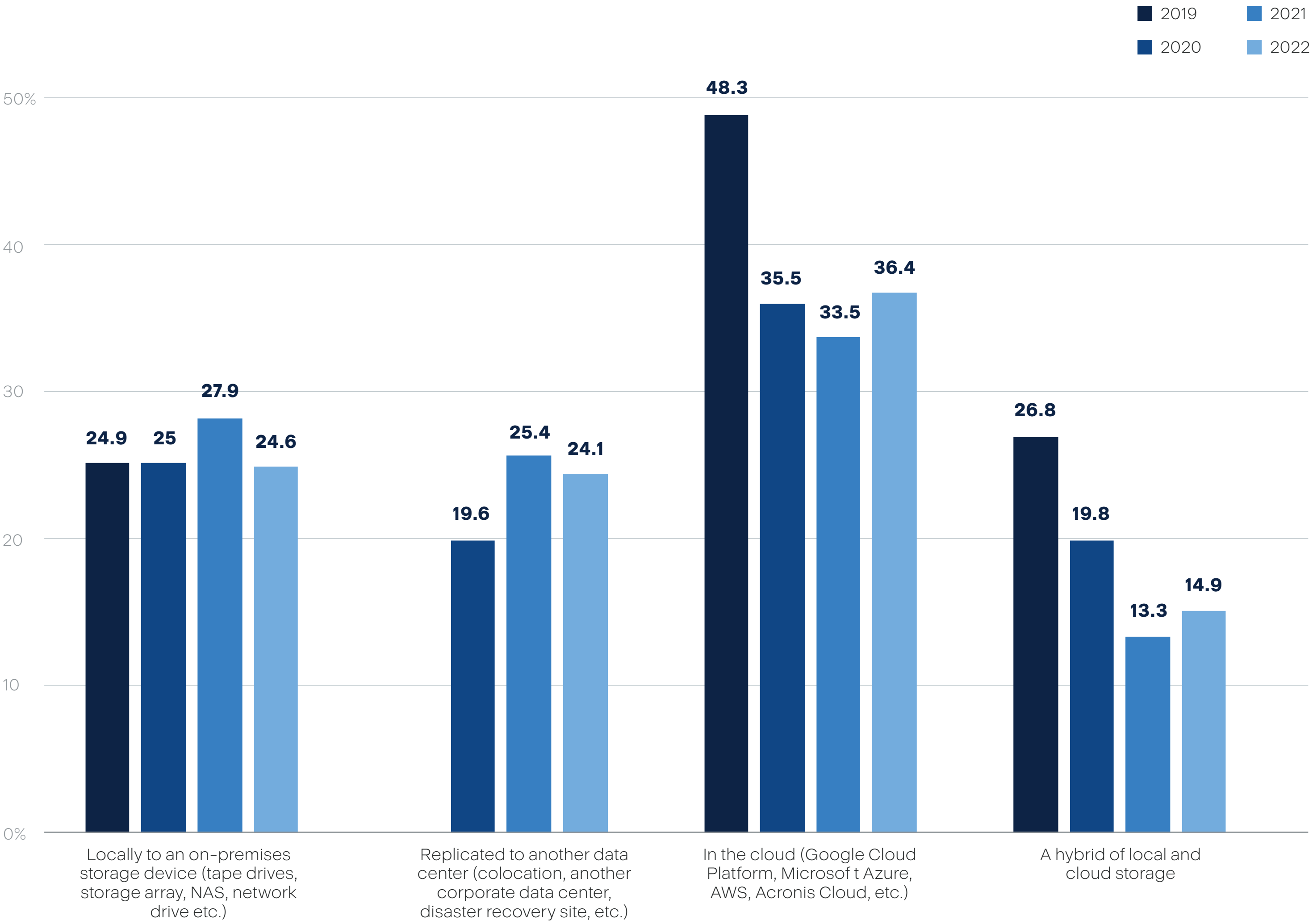
Driven by the pandemic, IT managers in 2020 and 2021 were backing up more, though not always better. This year that trend has come to an end.

Daily backups are down from 40% in 2021 to 21% this year. Weekly and monthly backups remain consistent, selected by 31% and 25% of IT managers respectively. We provided the IT managers with a new option this year, “multiple backups a day”. While this option is often the best practice for IT teams, just 18% of respondents reported backing up so frequently.

Overall, it seems the frequency of backups has decreased slightly — opening organizations to the loss of days or weeks of work when they need to recover from their most recent backup.

Just 15% of IT managers follow backup storage best practices

When you back up these devices, where do you back them up to?



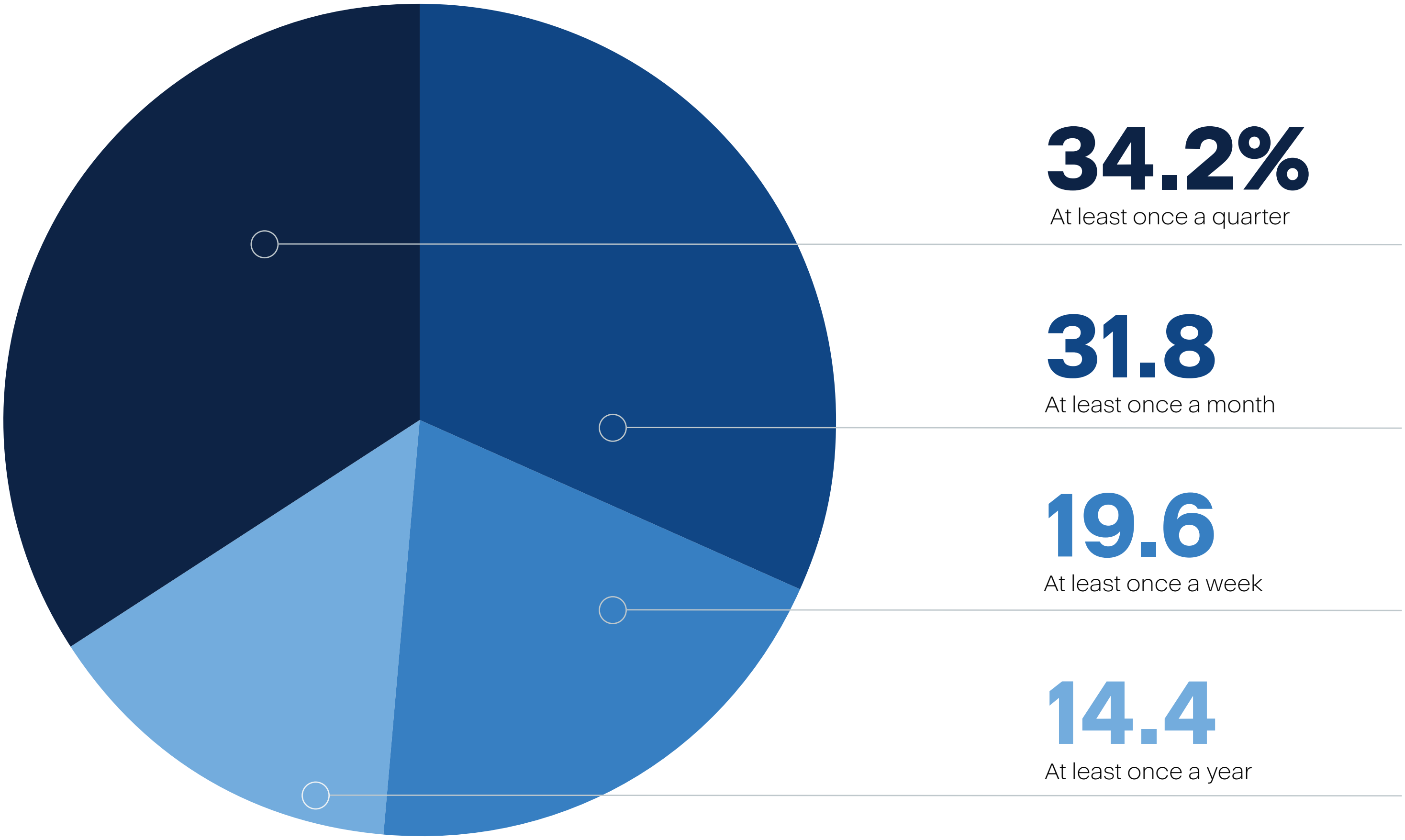
While cloud adoption gained a few points and holds at a steady rate of 37% in 2022, the best practice approach — a hybrid of local and cloud storage — has been in decline in the past few years. Down from 27% in 2019 to 15% this year, it showed only a minor improvement compared to 13% in 2021.

Straying away from the industry-established best practice 3-2-1 rule of backup suggests a reduced focus on data protection processes, which may open organizations to a greater risk of data loss and potential compliance issues.

Reality check: 20% of IT managers claim to be testing backup restoration weekly

#3

How often do you test your ability to restore IT environment components from a backup?



When asked how often they test the ability to restore from backup, 20% of IT managers globally claimed to be testing it weekly. However, based on the real-life external cases Acronis has examined in the past few years, we have to voice our doubts: in the best cases, we saw organizations performing monthly tests. More often than not, there was no testing in place at all.

While it's possible that some IT teams are improving in terms of testing and getting stricter — likely, having learned their lesson after suffering data loss last year — it's also entirely possible that IT professionals are simply maintaining appearances, since they are acutely aware that successful recoveries are key for their organizations' business continuity and productivity.

76% of companies suffered downtime in the past year — system crash, human error and cyberattacks among top causes

#4

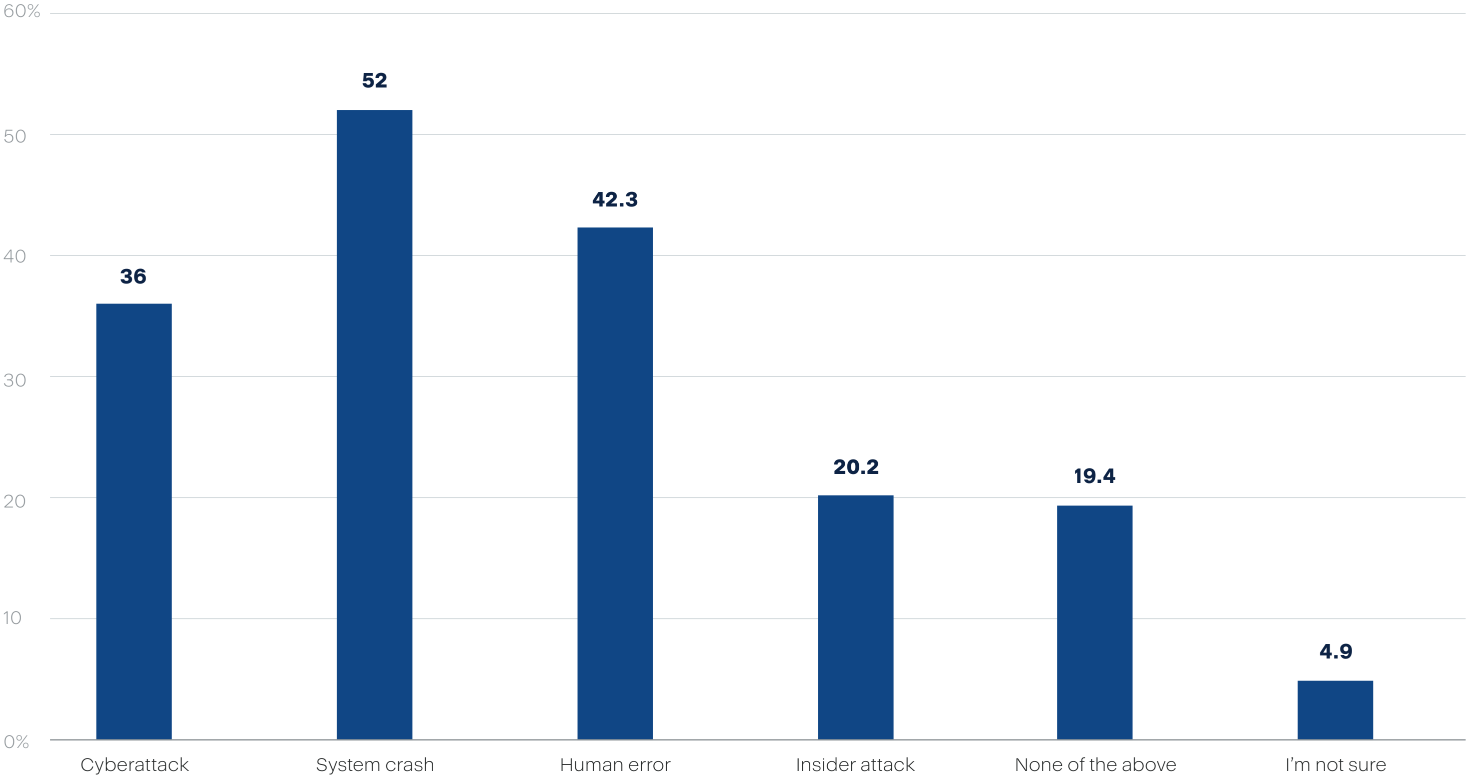
In the past year, has your organization experienced downtime due to any of the below?

Another worrying trend: the number of companies suffering downtime has skyrocketed. Our 2019 report saw 31% of IT managers experiencing downtime due to data loss, it rose to 49% in 2021. In the past year, 76% of organizations suffered downtime.

There are two potential explanations for this significant year-over-year growth: either the issue is getting worse or detection and reporting techniques are getting better — we believe both to be true.

The top three causes for downtime according to our research are consistent with other industry findings: system crashes, human error and cyberattacks. When tackling potential system crashes, IT teams should focus on backup/restore and disaster recovery overall. Investing in cybersecurity is the only way to tackle cyberattacks. As for human error, we recommend conducting regular employee training.

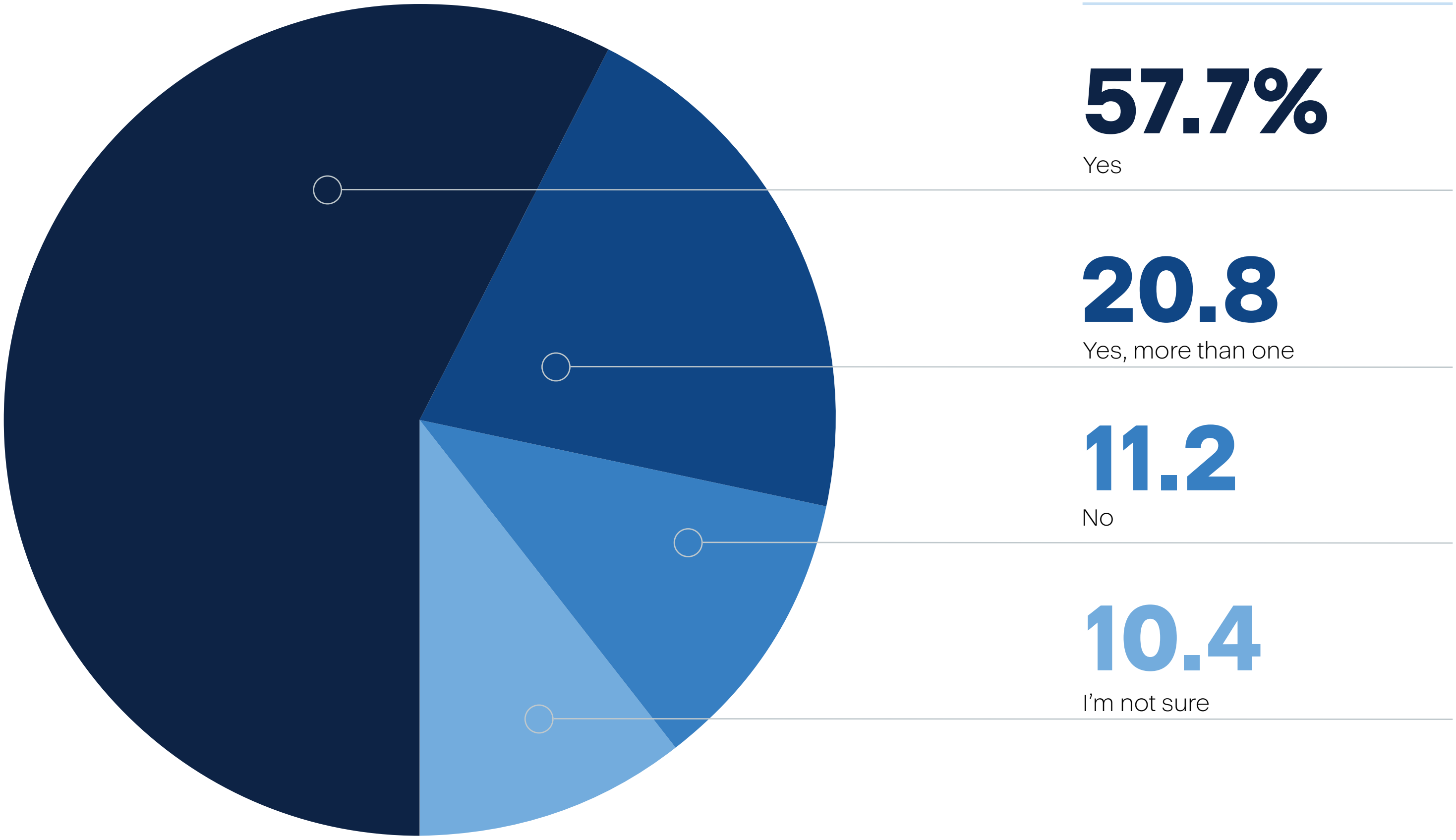
Tip: If your organization has a complex IT infrastructure or limited IT resources, check out Acronis Cyber Services — a support resource that handles the design, integration, implementation, backup, DR, storage, file sync and share and monitoring of your data protection solutions.



Confusion over data privacy regulations remains

#5

Is your organization currently subject to data privacy regulations?



Same as last year, 10% of IT managers aren't sure if their company is subject to any data privacy regulations. This goes to prove that IT managers ¬— same as IT users — get stuck in their ways.

Despite the growing geopolitical tensions and expanding data privacy regulations, compliance is still not a top priority for IT team. While the vast majority (78%) of IT managers report that they're subject to at least one data privacy regulation, 10% aren't certain.

If an IT manager doesn't know about the regulations they're subject to, they can't possibly meet the data privacy standards those regulations mandate.

The cyberthreat landscape is constantly evolving and cybercriminals continue to exploit a world in flux to attack more organizations than ever before. Only 20% of organizations reported that they didn't get attacked in 2021 — no wonder that IT managers are on high alert. The top five cyberthreats on their list remain consistent with our 2021 report. Our research shows, they have been taking steps to defend against those cyberthreats — but it's not all working out.

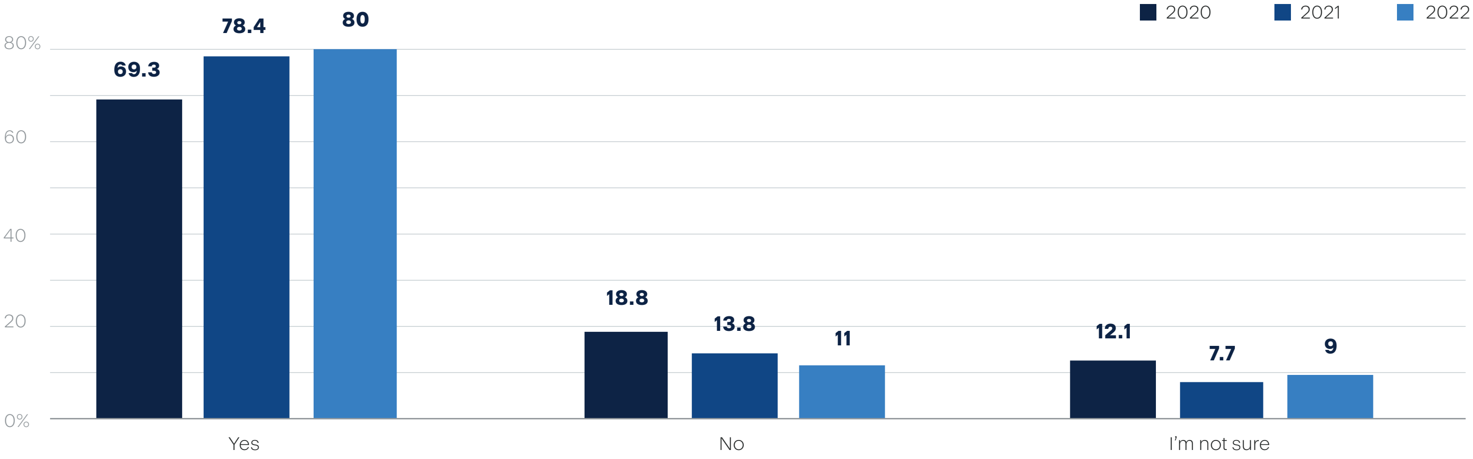
Top five cyberthreats that keep IT managers awake at night

Malware (virus, etc.) attacks	68%
Phishing attacks	65%
Business data theft / data breach	65%
Denial of service (DoS or DDoS) attacks	61%
Internet of Things (IoT) attacks / Ransomware (tied)	59%

More tools — yet, more companies suffer downtime each year

#6

Does your organization have a method in place to identify when data is unexpectedly accessed or modified?



Interestingly, while the number of companies equipped to detect when their data has been accessed or modified grows steadily each year (now at 80%) the number of companies suffering downtime reached an all-time high according to Cyber Protection Week report findings: 76% in 2022.

Overconfidence as a trend is both apparent and worrying — too many IT managers believe that having certain tools in place is enough protection, even when those tools are unintegrated, outdated and clearly ill-equipped to keep up with modern threats.

"More solutions" doesn't mean "more protection"

IT managers are still adding on more solutions — even though patchwork solutions don't work. Piling up unintegrated solutions doesn't increase protection and actually hurts efficiency and the overall efficacy of your defenses.

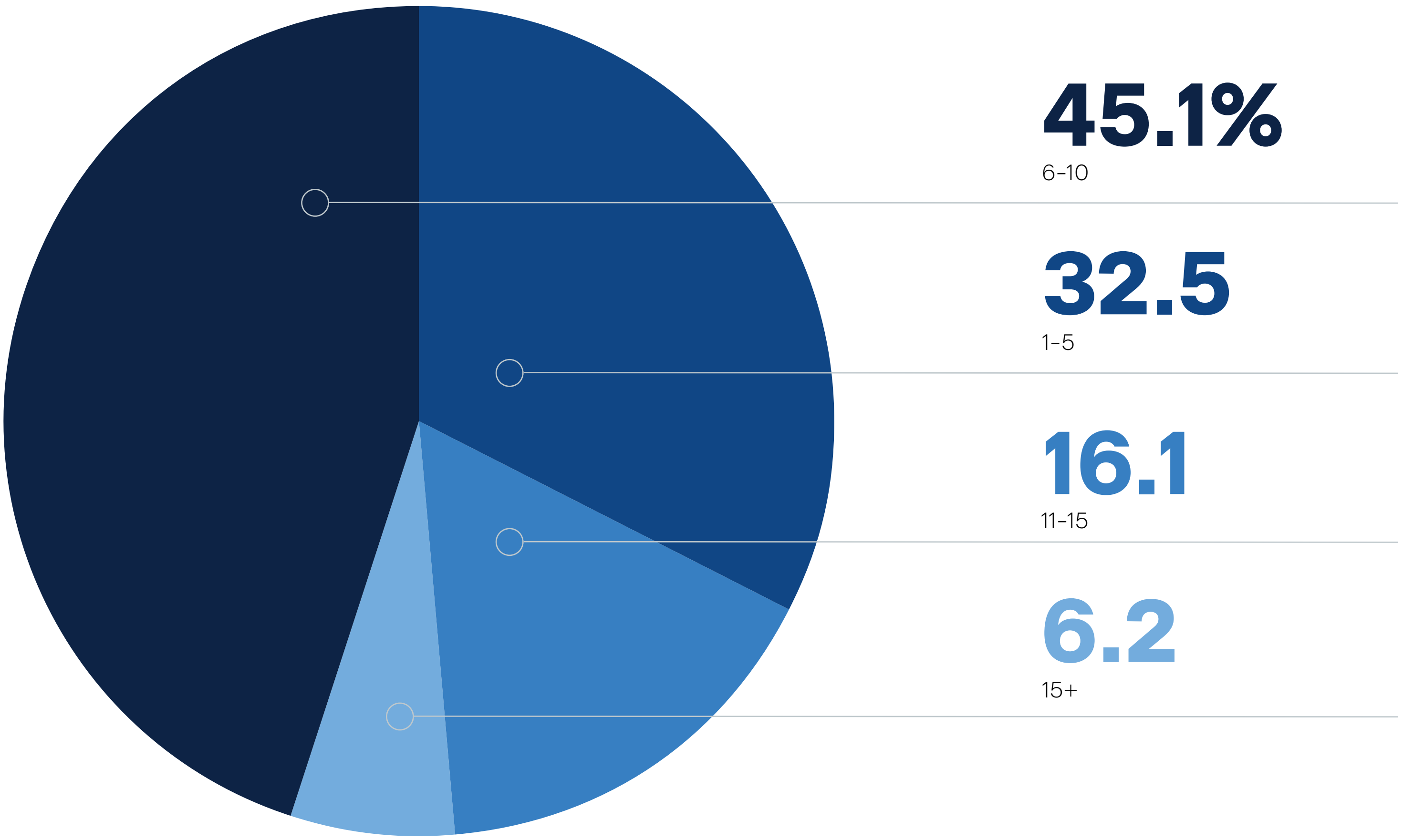
Does your organization have these cybersecurity technologies in place?

	Yes	No	I'm not sure
Ransomware protection and remediation	81.8%	11.6%	6.6%
Anti-malware with zero-day threat prevention capabilities	80.8%	13.0%	6.2%
Automated patch management	70.3%	20.4%	9.4%
Vulnerability assessments	73.5%	17.7%	8.8%
URL filtering	75.1%	17.9%	7.0%
Continuous data protection	81.2%	12.2%	6.6%
Endpoint detection & response / XDR	68.6%	19.3%	12.1%
Backup forensics	70.8%	19.4%	9.8%
Email security	85.1%	10.5%	4.5%
Data loss prevention	81.7%	12.0%	6.3%

#7

How many different security and protection tools and agents are you currently using?

Organizations have assembled highly complex patchworks of solutions: 78% of companies rely on up to 10 different services and agents to defend their data, applications and systems. Another 22% are using more than 10 different services. Unfortunately, this patchwork defense fails against modern IT challenges — such complexity only introduces costly mistakes.



Another contradiction in this year's results is with IT managers' responses as to the solutions they have enabled. 70% claim to have automated patch management — however, based on our observations, only a handful of companies follow the 72-hour "golden time" for patch management.

82% of respondents claim to have ransomware protection and remediation — yet, successful cases occur weekly and the size of ransom demands grows each year. Plus, IT managers still see ransomware as one of the top five cyberthreats. Similarly, 67% of IT managers report having endpoint detection and response (XDR), which is also unrealistic given the rate of data loss and cyberattacks.

The responses gathered on these points in this report do not align with Acronis or any industry-issued data. Patch management, DLP, XDR, backup forensics — all show nowhere near the high degree of adoption reported by our respondents. It would be optimistic to say that 20% of all companies can actually do backup forensics.

IT managers may be trying to seem better prepared than they are — potentially misleading their managers, boards of directors, industry analysts and customers.

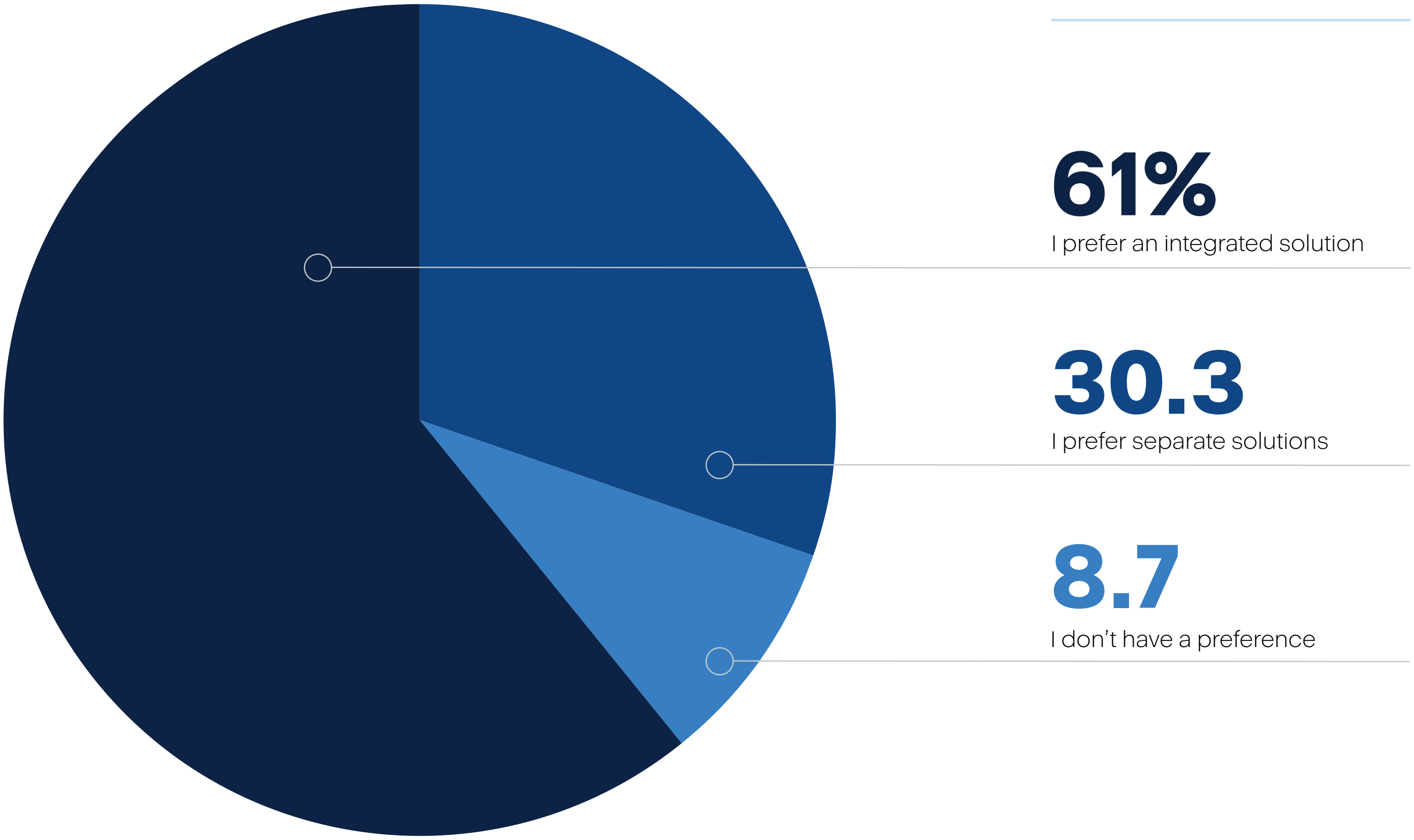
Alternatively, if the overwhelming majority of IT managers do have these solutions, they aren't getting the level of protection they had planned for. To defend against data loss and cyberthreats, they have stocked their IT stacks with all of the recommended cybersecurity technologies — to no avail.

Tip: Learn more about detection and response here. Solutions designed for zero trust, detecting and stopping suspicious activities, with real-time visibility, automatic and manual remediation.

#8

61% of IT managers see the need for an integrated backup and security solution

Do you prefer an integrated backup and security solution or separate backup and security solutions?



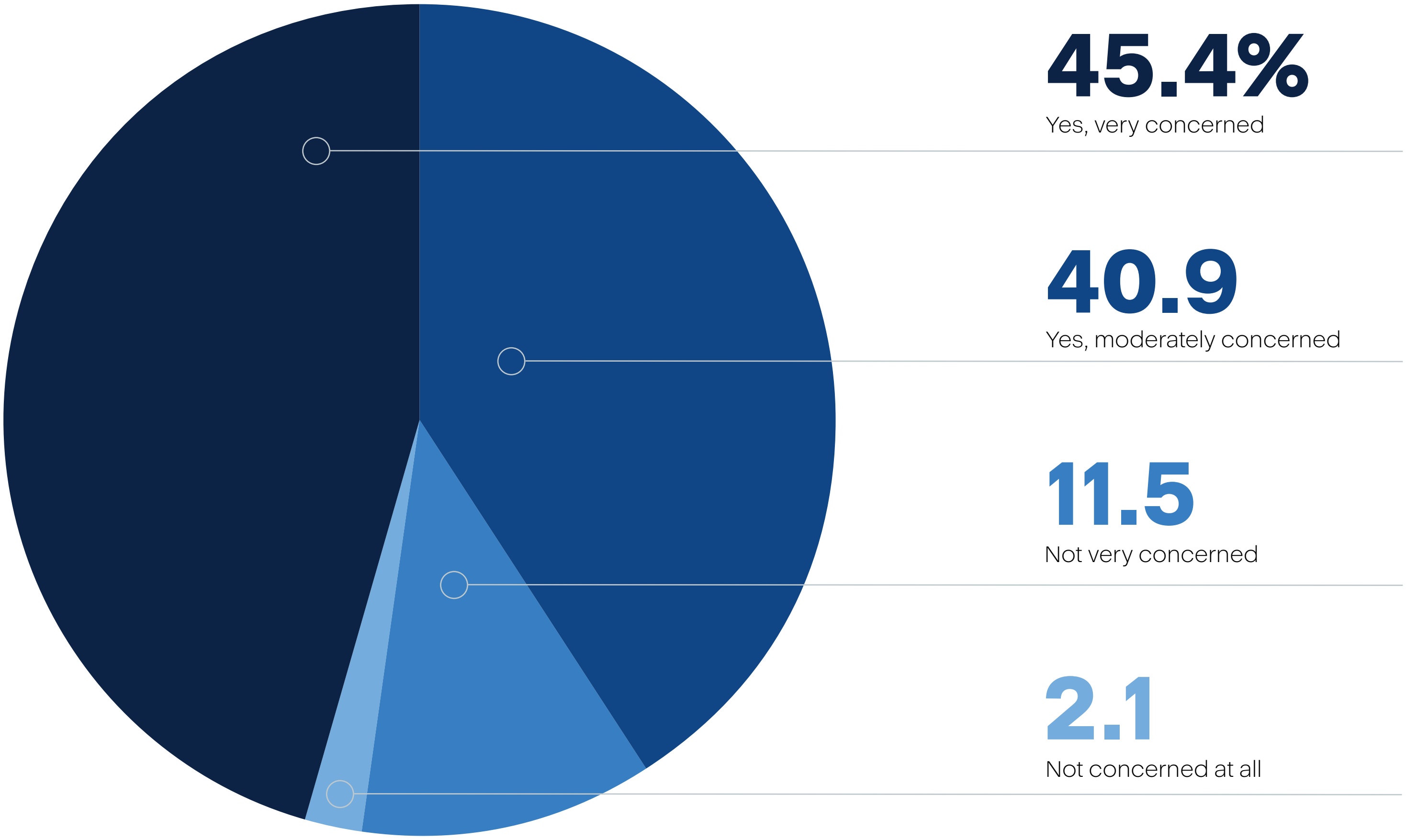
Perhaps because of this gap between the investment IT managers are making in their security posture and the efficacy of their solutions, the majority of IT managers (61%) prefer an integrated backup and security solution. This suggests a major move in the industry, as more IT professionals than ever are appreciating the benefits and importance of the integrated cyber protection approach.

30% of IT managers are either slow to evolve or have certain restrictions preventing them from switching to integrated solutions. Either way, sticking with outdated methods will prove disastrous for any organization.

86% of IT managers are concerned about the increasing politically-driven cyberattacks

#9

Are you concerned about increased cyberattacks caused by the current geopolitical climate?



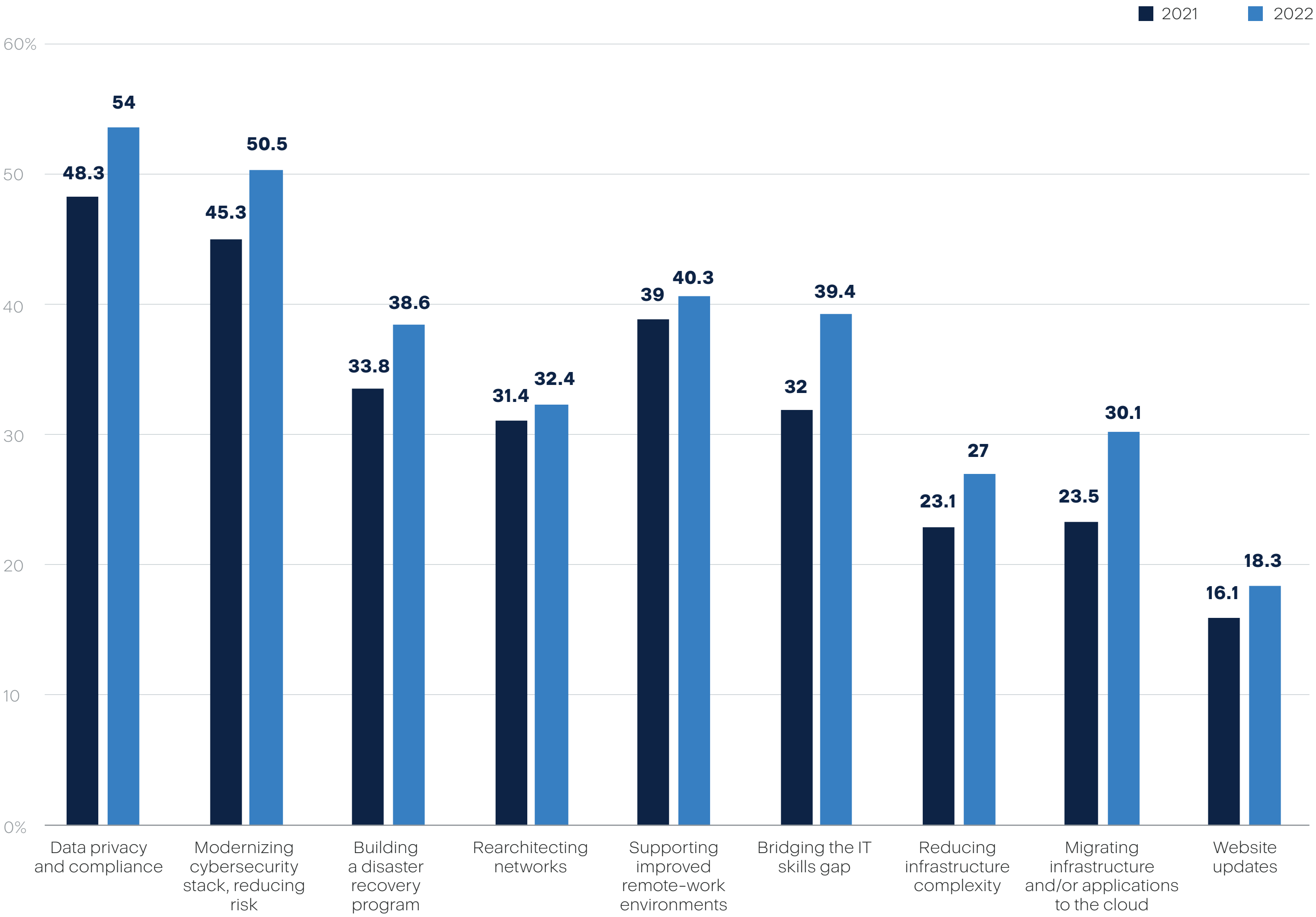
With 86% of IT managers concerned about the current geopolitical climate and its impact on cyberthreats, why should businesses care about attacks targeting public sectors? While the attacks on public sector get vast coverage — think of the WannaCry and SolarWinds supply chain attack — truth is, there are many more attacks on SMEs. They're successful attacks too, but they aren't as present in the headlines. Attackers do not discriminate when it comes to who they attack and businesses store large volumes of sensitive and personal data about clients and employees, which is useful information for any attacker looking to scope out future targets.

Tip: Data Magic Computer Services: 71% of ransomware attacks are targeting small businesses

More tools – yet, more companies suffer downtime each year

#10

Does your organization have a method in place to identify when data is unexpectedly accessed or modified?



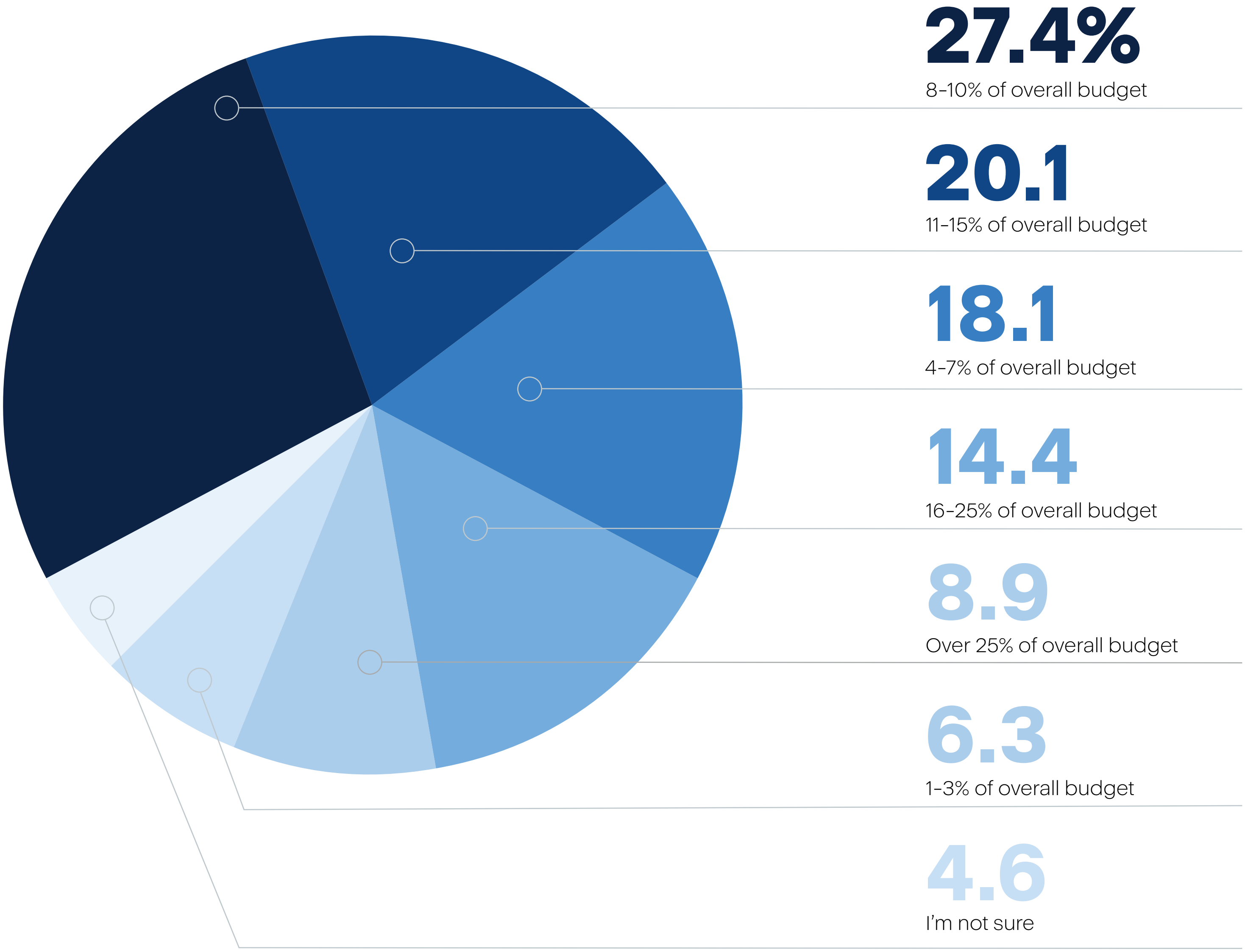
To confront these challenges, IT managers are pursuing a wide variety of IT improvements and enhancements in the year ahead — investing more across the board in 2022. Their top priorities include: data privacy and compliance; modernizing cybersecurity stacks to reduce risk; supporting improved remote-work environments and bridging the IT skills gap. Reducing infrastructure complexity is also showing some growth — 27% of IT managers intend to simplify their infrastructure in 2022, which will end up saving them money when replacing the patchwork of 10+ IT solutions they rely on now.

Privacy and compliance earned the top spot for the second year in a row, which is interesting given that 22% of organizations claim they either aren't subject to any regulations or aren't aware of any data privacy requirements that affect them.

Half of organizations allocate less than 10% of their IT budget on IT security

#11

What percentage of your company's IT budget is spent on IT security?



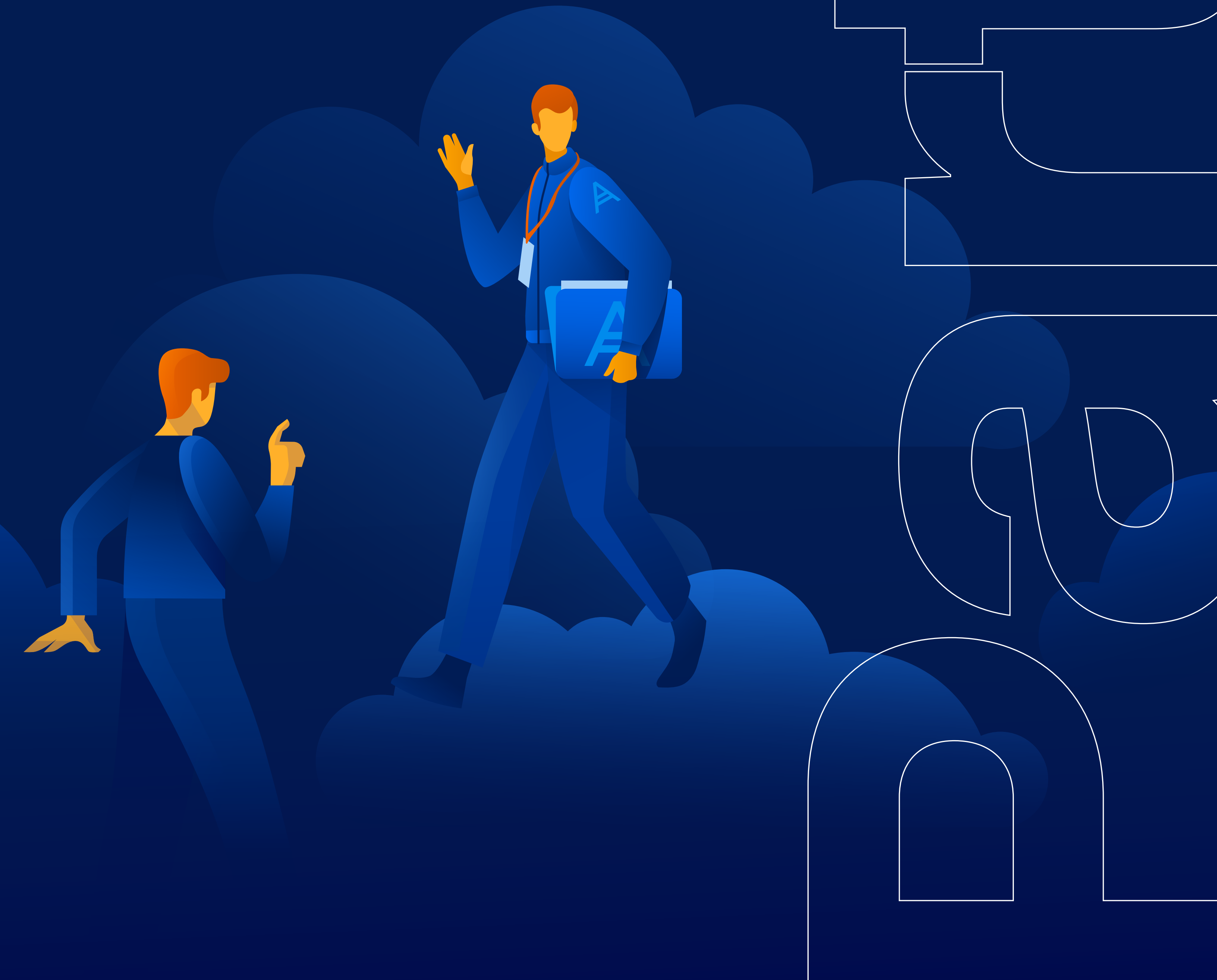
Only 23% of companies are investing over 15% of their overall IT budget into security — despite the ever-growing cyberthreats and numerous concerns expressed by IT managers.

As a cyber protection company, we commend investing in security, but it's important to spend wisely — instead of just building a stack of unintegrated, outdated solutions. As 2022 will continue to prove further, the best way to utilize this budget is with integrated solutions.

Key takeaways

While awareness of the cyberthreats continues to grow, it's obvious there is a massive gap in how organizations and individuals approach cyber protection, both in theory and in practice.

Part 3



At home and at work, today we’re more dependent than ever on the digital world. Yet some companies are a single DDoS attack away from their whole business coming to a halt. In another example, over 5,800 wind turbines in Central Europe lost connectivity to their uplink satellite connection in early 2022, rendering them unmanageable. Events like these prove the need for comprehensive protection and continuity plans.

Having up-to-date and tested backups of all your important data and a disaster recovery strategy can greatly minimize your business’ downtime. No matter if your data center is physically damaged, the connection is lost or a cyberattack wiped all your data clean, it helps if you can quickly switch to a different site and restore efficiently in the background.

The outdated approaches that IT users and professional IT teams have relied on for years are now actively failing them. A comprehensive, easy-to-follow approach is essential to achieving a more reliable, holistic defense for data, applications and systems.

To see if you’re equipped for the challenges and cyberthreats in the year ahead, ask yourself if your personal or professional cyber protection solutions:

- Reduce complexity?
- Streamline protection and management?
- Connect disparate capabilities?
- Inform users about the status of their defenses?

If they don’t — then it’s time for an upgrade.

Upgrade now

About Acronis

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions powered by AI. With advanced anti-malware powered by cutting-edge machine intelligence and blockchain based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 2,000 employees and offices in 34 locations worldwide. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, and top-tier professional sports teams. Acronis products are available through over 50,000 partners and service providers in over 150 countries and 26 languages.