Acronis

Acronis Cyber Protection Week Global Report

Acronis
Cyber Protection Week
Global Report 2021

Table
of contents

Introduction and research methodology

Data reliance has grown to new heights in recent years, yet the technologies and processes that are used to keep IT systems safe and secure haven't kept pace. To raise awareness of this gap in protection, last year Acronis expanded World Backup Day – the annual holiday celebrated on March 31 as a reminder to back up data – to Cyber Protection Week.

This shift came with research from the world leader in cyber protection that illustrated the shortcomings that individuals and organizations faced when trying to keep up with modern IT needs through the use of traditional data protection and cybersecurity strategies and solutions.

Expanding this effort even further in 2021, Acronis conducted independent research, surveying 4,400 IT users and professionals from 22 countries. The findings of this research provide a wealth of insight into:

- How individuals and organizations are approaching the modernization of their IT defenses
- What gaps remain in modern protection strategies
- How cybercriminals are looking to exploit those gaps
- How internal IT teams and external IT service organizations can prepare for and overcome them

ABOUT THE SURVEY METHODOLOGY

Acronis surveyed 4,400 IT users and professionals to learn about their unique experiences and perspectives with today's cyber protection solutions and cyberthreat landscape. Acronis had no role in selecting the respondents. All responses were provided anonymously. The survey was conducted in March 2021.

Respondents came from 22 countries across six continents: US, Canada, Mexico, Brazil, Australia, India, South Korea, Singapore, Japan, Germany, Switzerland, UK, Belgium, Netherlands, Sweden, France, Italy, Spain, Bulgaria, Saudi Arabia, UAE, and South Africa.

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

KEY INDUSTRIES REPRESENTED IN THE IT PROFESSIONAL SEGMENT OF THE SURVEY INCLUDE:

IT/Telecommunications

Healthcare

Business services (Financial, Legal, etc.)

Manufacturing

Executive summary

KEY RESEARCH FINDINGS

Investing in more solutions doesn't mean more protection

To protect business data, applications, and systems – particularly during the pandemic's shift to remote work environments – organizations added new solutions to their IT environments. It's not working.

- ~75% of IT professionals report that their organizations have all recommended cybersecurity technologies in place

- 80% of organizations have up to 10 different protection and security tools running simultaneously

- Despite this, securing remote environments, ensuring availability, and maintaining employee productivity are still top challenges for IT pros

- More than half of organizations saw downtime due to data loss last year

A lack of awareness is creating a lack of protection

Significant gaps in awareness regarding cybersecurity and technology capabilities are costing individuals and organizations time, money, and security.

- Just 13% of IT users and IT professionals follow backup best practices

- 68% of IT users and 20% of IT professionals wouldn't know if their data had been unexpectedly modified because tools don't make it easy to find out

- 43% of IT users don't know if their anti-malware stops zero-day threats because it's not easy to find out

- ~25% of IT users don't know what ransomware, cryptojacking, Dos/DDoS, and IoT attacks are

- 10% of IT pros don't know if they're subject to data privacy regulations, risking major fines for potential compliance violations

IT users don't feel accountable for the protection and security of their data and devices

Personal reliance on technology continues to grow but efforts to protect that technology aren't keeping pace, likely due to false assumptions and reliance on automatic solutions.

- 83% of IT users spent more time on their devices last year. Only half of them took extra steps to protect those devices.

- 1/3 of IT users don't update their devices until at least a week after being notified

- While 90% of IT users perform backups, 73% have irretrievably lost data at least once, suggesting that they don't know how to back up or recover properly

- Patch management and vulnerability assessment tools that would simplify cybersecurity see low adoption

IT users

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

- When you back up your devices, where do you back up to?

- Have you ever had to recover from a backup?

- How long did it take to restore your system?

- Have you or a family member ever permanently lost data from a computer or mobile device?

- How concerned are you about the following cyberthreats?

- What steps have you taken to protect your privacy online?

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

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

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

- In the last year did you use your devices more than usual (due to pandemic lockdowns, remote work, etc.)?

One in ten people don't see data loss as a problem

How often do you back up your computer and mobile devices?
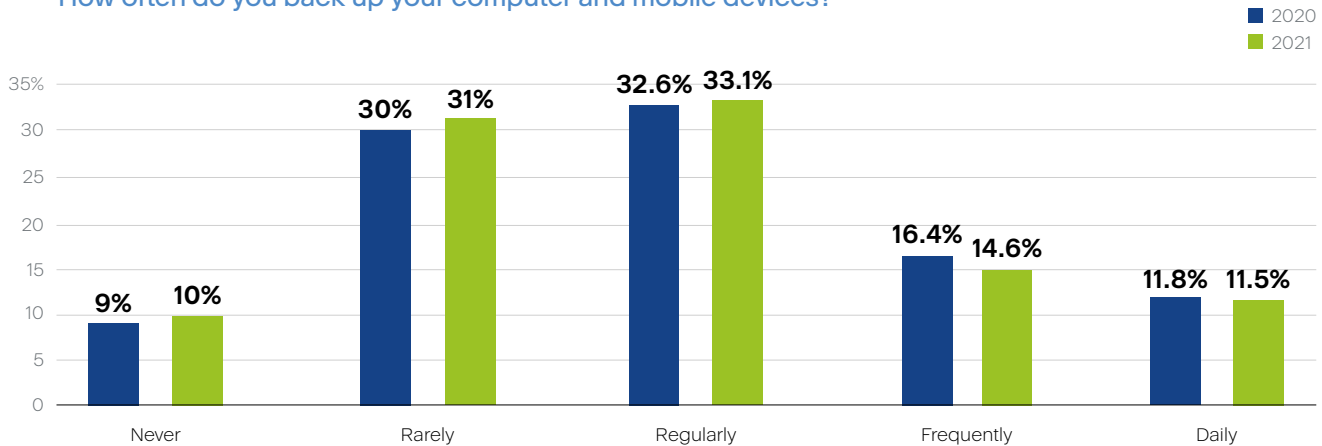
Backup habits are consistent from last year's Cyber Protection Week research. 10% of individual users never back up – half of them falsely thinking that they don't have to do so while the other half cite complexity, cost, and backup time requirements as their rationale. Regardless of their reason, these people feel that data loss is either unlikely to affect them or unlikely to be an issue if it does.

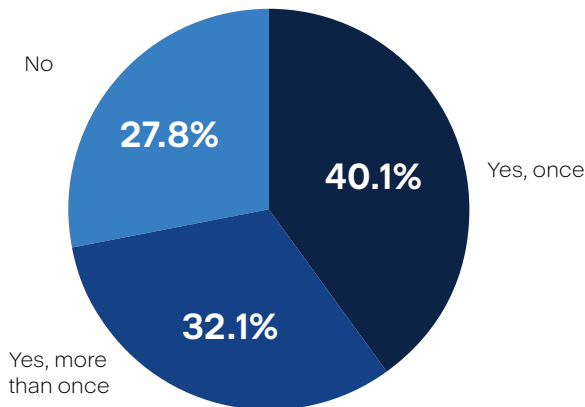# Use of backup best practices is declining

When you back up your devices, where do you back up to?
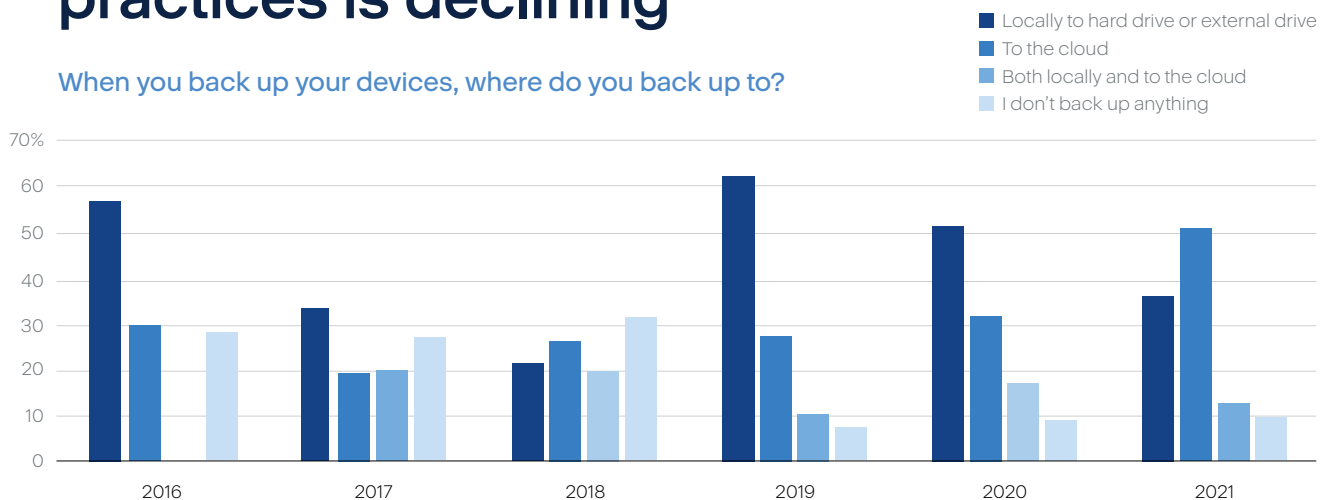
When backing up, personal IT users count on the cloud more than ever – up 20% over last year's response. Part of this growth is likely because public cloud solutions perform backups automatically, an example of broader automatic protection features that our report suggests individuals and organizations are depending on more and more. At the same time, just 13% of IT users use the hybrid local and cloud backup strategy that the IT industry has long considered a best practice for data protection.

Recoveries are common – and cost a lot of time

Have you ever had to recover from a backup?

No 27.8%

Yes, once 40.1%

Yes, more than once 32.1%

How long did it take to restore your system?

6.1% More than 24 hours

Up to 24 hours 15%

Up to an hour 32.7%
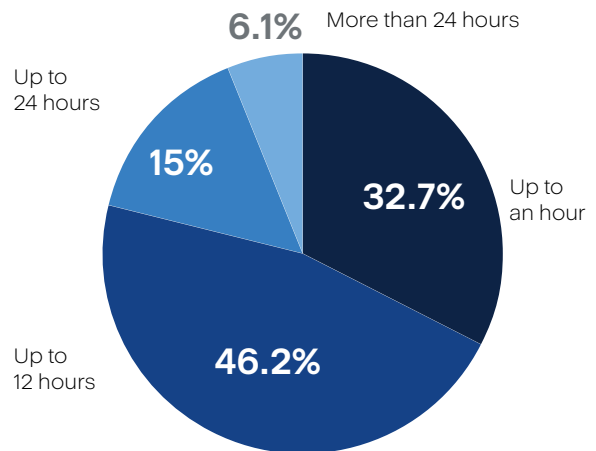
Up to 12 hours 46.2%

It's good that 90% of IT users back up their data because nearly 75% of personal IT users have had to rely on backups to recover lost data. That said, when performing those recoveries 79% of IT users spend up to 12 hours trying to regain access. This suggests issues with the recovery process, which may stem from unfamiliarity with the technology or issues with the way the backup was performed.

Despite backups, irretrievable data loss is a familiar experience

Have you or a family member ever permanently lost data from a computer or mobile device?
(Accidental deletions, app/system crashes, malware attacks, lost/stolen device, etc.)

Nearly 75% of personal IT users have had experience permanently losing data. This loss may have inspired more people to back up their devices, but given that this figure is up by nearly 10% over last year, it's just as likely that these moments of irretrievable data loss result from a combination of infrequent backups and ineffective recovery processes.

- Yes
- No

80%
70
60
50
40
30
20
10
0

2019   2020   2021

www.acronis.com
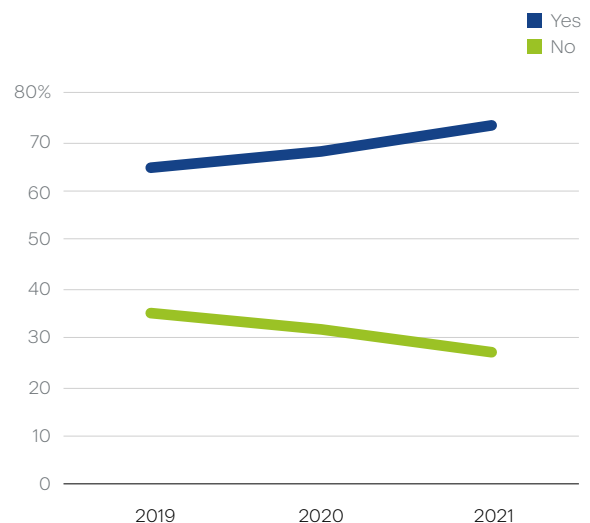
Looming cyberthreats aren't on the radar

How concerned are you about the following cyberthreats?

Percentage of personal IT users unfamiliar with cyberthreats

CYBERTHREAT	2020	2021
Ransomware	17%	22%
Cryptojacking	22%	27%
Data Theft	11%	4%
Phishing Attacks		11%
DoS / DDoS Attacks		24%
Malware		7%
IoT Attacks		20%

According to the FBI, cybercrime grew by 400% in the past year. Nearly every week, headlines included stories of data breaches and ransomware. Despite all of this coverage, nearly 25% of personal IT users aren't familiar with ransomware, cryptojacking, Denial of Service (DoS / DDoS) attacks, or IoT attacks. This speaks to a shocking lack of awareness on the part of personal IT users that may stem from the false belief that cyberattacks aren't a threat for individual users – a belief that has been proven incorrect countless times.

Efforts to ensure online privacy don't reach far beyond common sense steps

What steps have you taken to protect your privacy online?

Individual IT users are protective of their privacy online, though the steps they're willing to take to defend their privacy don't go much farther than basic – often automatically encouraged – steps like the use of strong passwords, secure Wi-Fi connections, and app-driven defenses like multi-factor authentication and cloud backup storage. Going beyond these efforts is much less likely because it would require proactive steps and consistent awareness about evolving and emerging cyberthreats.

A lack of awareness is threatening personal data protection

Would you know if any of your data had been unexpectedly accessed or modified?
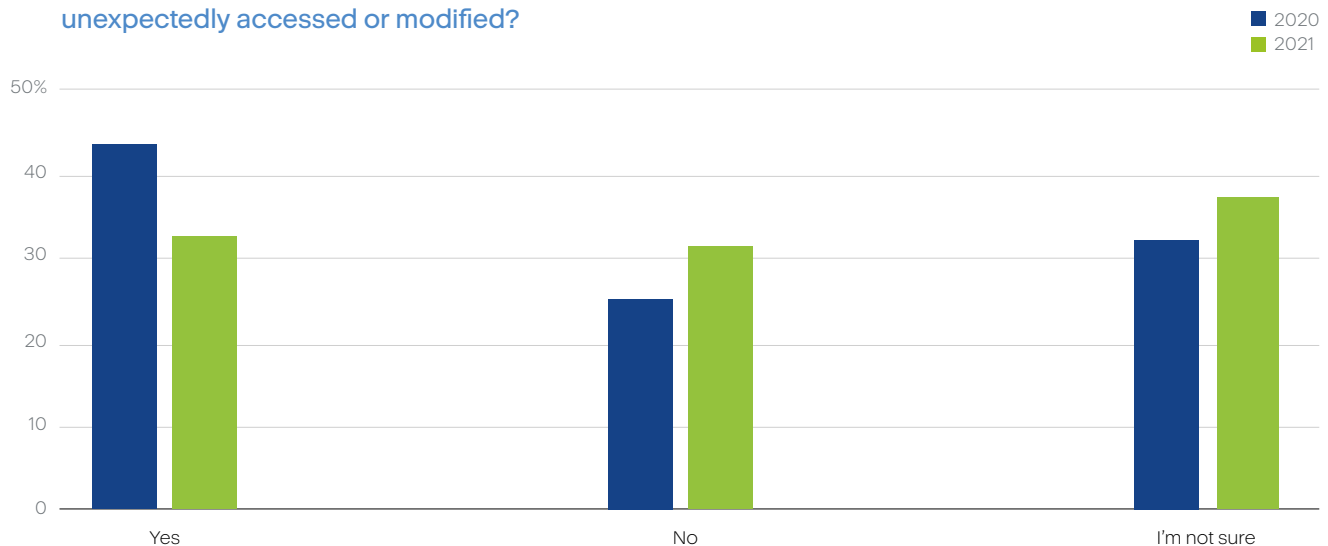
Does your anti-malware protect against never-before-seen (zero-day) cyberthreats?
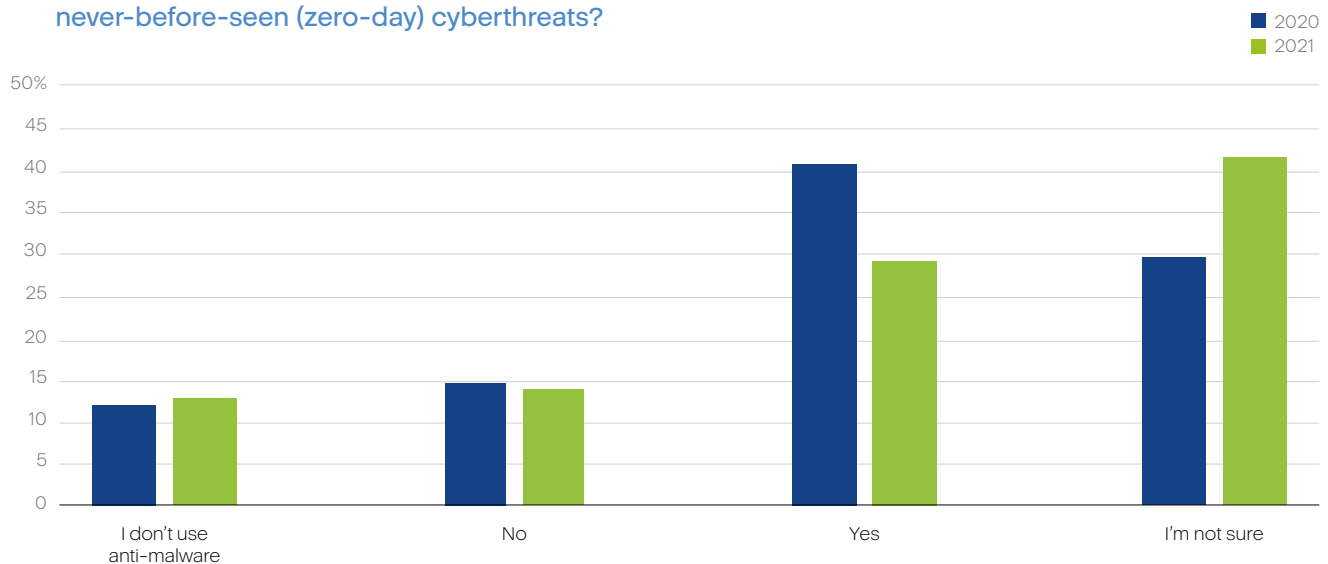
A lack of awareness is on the rise among personal IT users. Nearly 40% wouldn't know if their data was unexpectedly accessed or modified – up 10% from last year – and even more don't know if their anti-malware would stop zero-day threats. This poses a serious threat because a lack of knowledge can easily lead to a lack of preparation and security.

And, given that IT analysts report 350,000 new malware threats every day – this knowledge gap is primed to be a threat that only grows over time, making increased protection awareness and engagement even more important.

Accountability over data protection and security isn't keeping pace

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

5% More than a month later

Within a month

6.3%

Within a week

22.3%

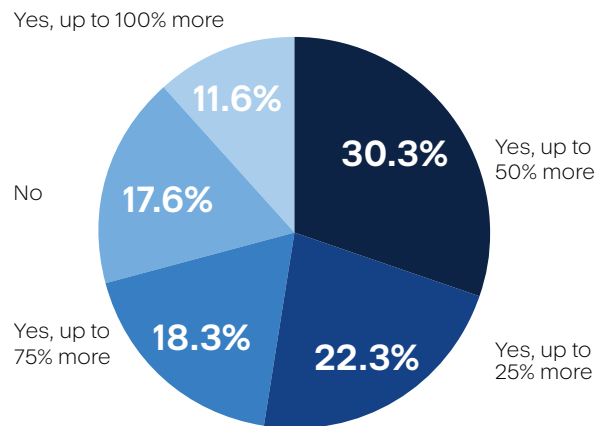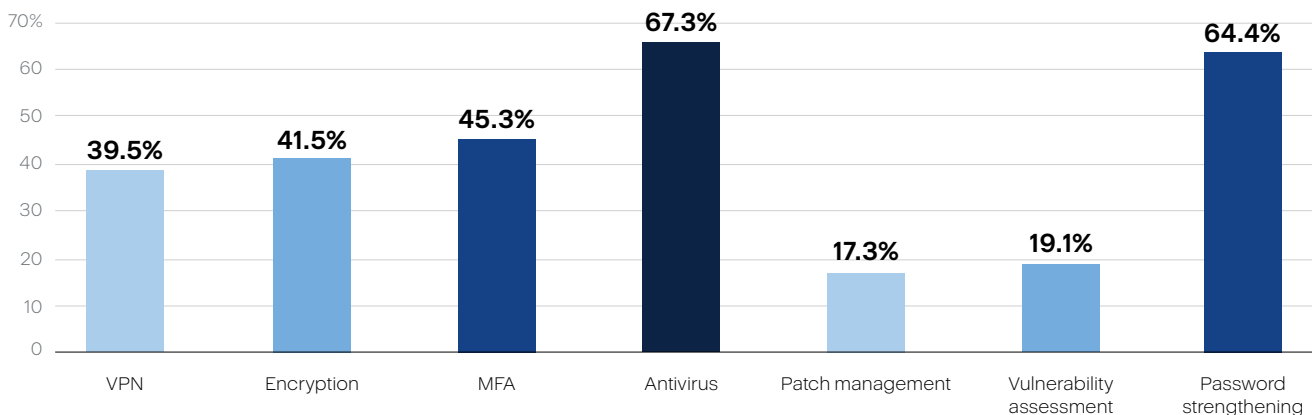**37.9%** Within a day

Within an hour

28.5%

In the last year did you use your devices more than usual (due to pandemic lockdowns, remote work, etc.)?

Yes, up to 100% more

11.6%

No

17.6%

30.3% Yes, up to 50% more

Yes, up to 75% more

18.3%

22.3% Yes, up to 25% more
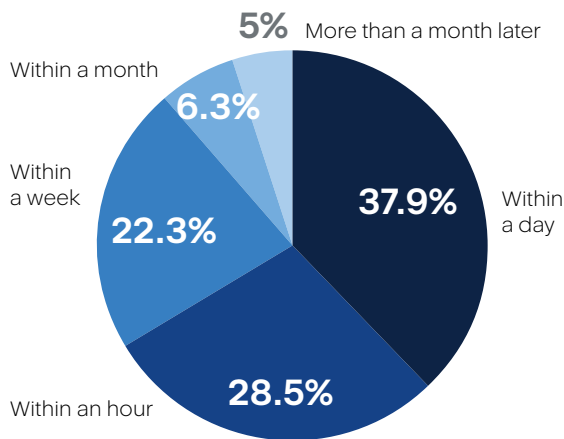
What extra precautionary steps did you take? Select all that apply:

Category	Value
VPN	39.5%
Encryption	41.5%
MFA	45.3%
Antivirus	67.3%
Patch management	17.3%
Vulnerability assessment	19.1%
Password strengthening	64.4%

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. Particularly of note, 78% of personal IT users report that they're using their devices more since the beginning of the COVID pandemic but only half of them are doing more to protect those devices. That means half of the personal devices that IT users rely on are open to more risks, threats, and vulnerabilities without any extra defenses put in place – an opportunity that cybercriminals will be drawn to exploit.

This opportunity is made even more enticing for cybercriminals given that one-third of personal IT users take a week or more to patch vulnerabilities after they're notified that one is available. Of those, 5% take longer 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 patches.

IT professionals

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

- When you back up your devices, where do you back up to?

- When backing up, do you treat all devices the same in terms of scheduling, recovery testing, etc.?

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

- Is your organization currently subject to data privacy regulations?

- How would you rate your organization's concern regarding these cyberthreats?

- Does your organization have these cybersecurity technologies in place?

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

- In the past year, has your organization experienced data loss that resulted in downtime?

- In the last year did your organization shift to increased remote working environments?

- What has been the biggest IT challenge your organization faced during and following the shift to remote work?

- What IT projects are you prioritizing in the year ahead?

- Is your company planning to spend more to meet those IT challenges in 2021?

# More IT pros are performing backups. Frequency remains consistent

How often do you back up the IT environment components your organization is responsible for (servers, endpoints, mobile devices, etc.)**?**

■ 2019
■ 2020
■ 2021
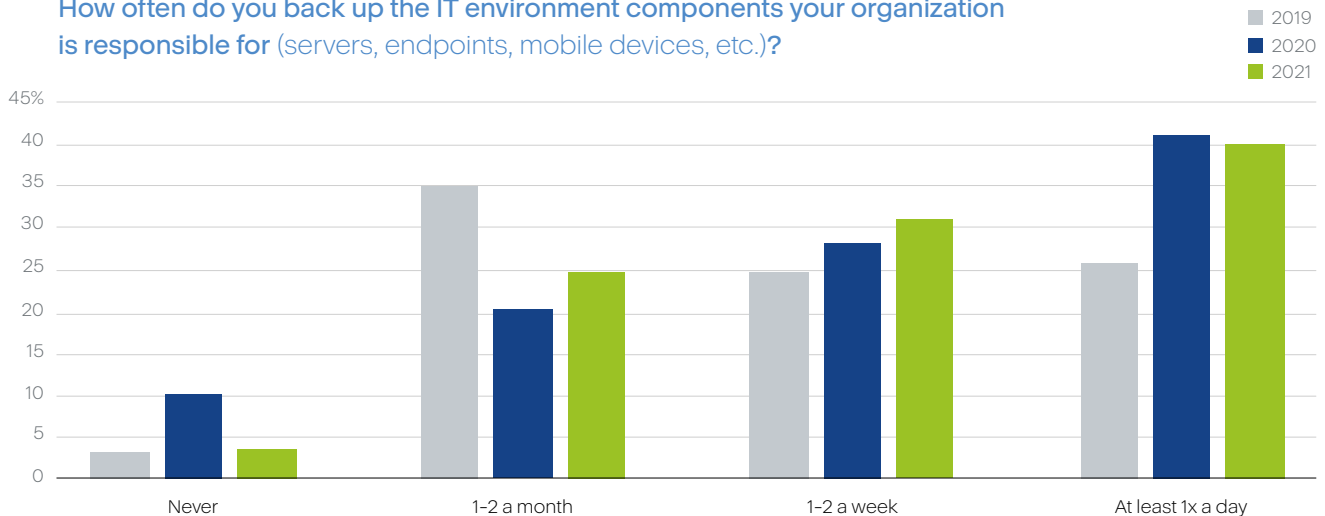
The percentage of organizations that don't back up data saw a significant drop from 2020. This could stem from developments in the past year including increased awareness of data loss consequences, increased remote working, and expanded data privacy regulations. That said, the frequency of those backups has not increased, opening organizations to the loss of days or weeks of work when they need to recover from their most recent backup.

Use of backup best practices is declining

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

■ 2019
■ 2020
■ 2021
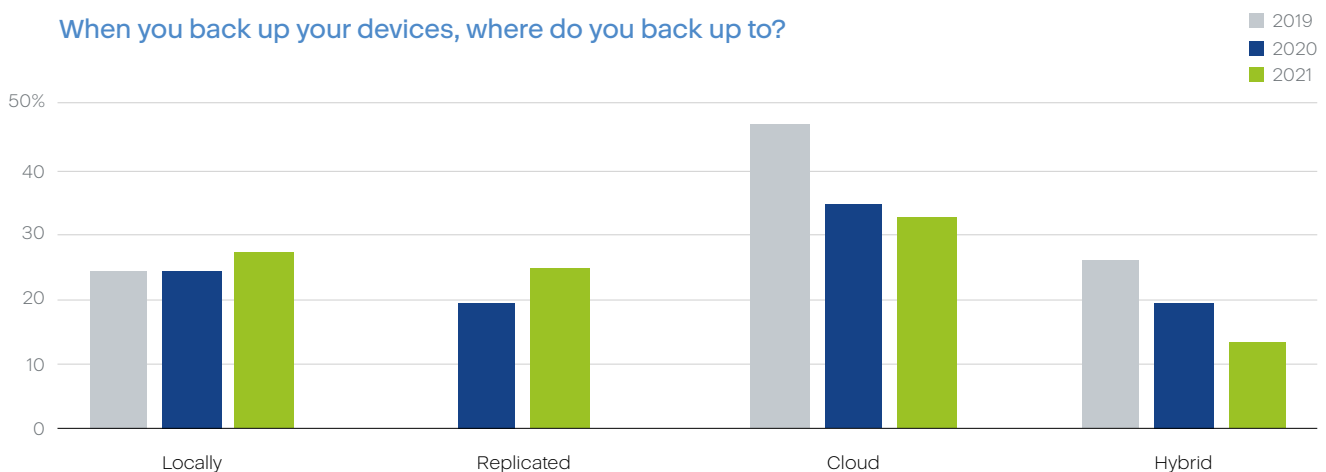
Making matters worse, IT professionals who perform backups are straying away from the industry-established best practice 3-2-1 rule of backup. Only 13% still adhere to this hybrid policy, down from last year's 20%. This suggests a reduced focus on backup and data protection processes, which may open organizations to a greater threat of data loss and potential compliance issues – as demonstrated by recent headline-grabbing incidents like the OVHcloud fire.

Organizations lack backup sophistication

When backing up, do you treat all devices the same in terms of scheduling, recovery testing, etc.?

Shockingly, less than half of the surveyed IT professionals customize and prioritize their backup processes, instead applying an unsophisticated, universal approach that places servers full of data on the same level of importance as an end user's laptop. Given that backup prioritization is a widely available capability, this approach implies that most organizations view backups as a box to be checked without diving deeper into ways data protection could be optimized to ensure the most efficient recoveries when they're needed.

6.6% No, device type prioritization

No, user prioritization

18.0%

56.6% Yes

18.9%

No, application prioritization
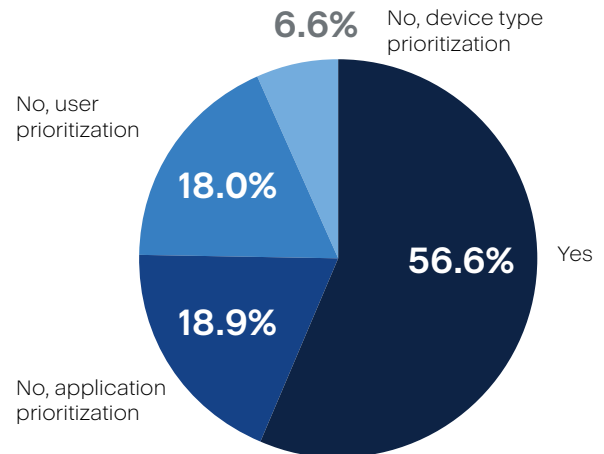
Despite basic backup processes, recovery is top-of-mind

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

Despite reduced adherence to backup best practices and process sophistication, IT professionals are acutely aware that successful recoveries are key for their organizations' business continuity and productivity. For most IT pros, recovery tests are performed at least once a quarter – with a significant segment accelerating this process and performing three to twelve tests in that same period.

At least once a year

At least once a quarter

14.0%

At least once a week

At least once a quarter

15.9%

38.6%

At least once a month

31.4%
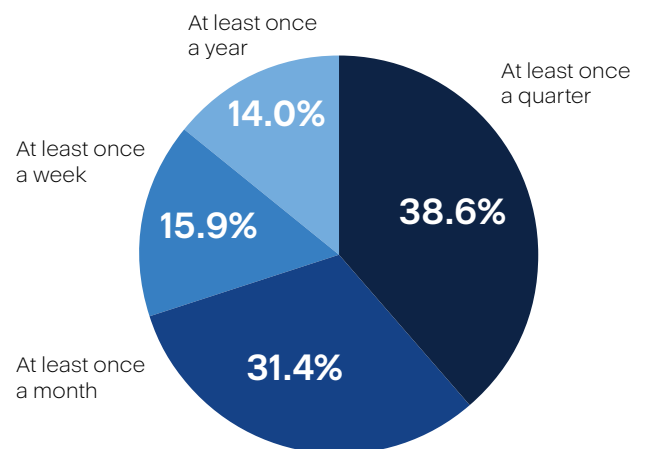
Confusion over data privacy regulations is on the rise

Is your organization currently subject to data privacy regulations?

Interestingly, compliance doesn't seem to share the same top-of-mind position that data recovery processes do. While the vast majority of IT professionals report that they're subject to at least one data privacy regulation, 10% aren't sure. That's 5% more than claimed ignorance in 2020. Of course, if an IT professional doesn't know about the regulations they're subject to, they can't reliably meet the data privacy standards those regulations mandate – creating a dangerous and potentially costly gap in both awareness and capability.

I'm not sure **9.7%**

No **12.6%**

56.9% Yes

Yes, more than once **20.8%**
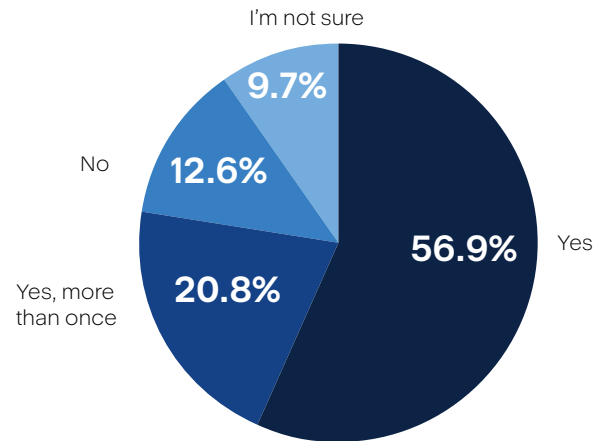
The cyberthreats keeping IT pros up at night

What cyberthreats are you most concerned about?

2020	2021
Data Theft	Malware
Ransomware	Data Theft
Social Engineering	Phishing
	DoS / DDoS
	IoT Attacks
	Ransomware
	Insider Attacks
	Cryptojacking

The cyberthreat landscape is constantly evolving and in the past year cybercriminals exploited a world in flux to attack more organizations than ever before. Nearly one-third of organizations were attacked on a daily basis in 2020. It makes sense, then, that IT professionals are concerned about all of the cyberthreats that threaten organizations today. And, as our research shows, IT pros are taking steps to defend against them all – though with mixed success.

A complex patchwork of defenses

Does your organization have these cybersecurity technologies in place?

	Yes	No	Not sure
Ransomware protection and remediation	78.8%	14.8%	6.3%
Anti-malware with zero-day threat prevention capabilities	78.4%	14.9%	6.7%
Automated patch management	67.4%	21.7%	11.0%
Vulnerability assessments	72.1%	20.0%	7.9%
URL f iltering	74.8%	17.5%	7.7%
Continuous data protection	79.8%	13.9%	6.3%
Hard drive health monitoring	75.7%	17.4%	6.9%
Backup forensics	68.3%	22.0%	9.7%

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

- 7.2% — 15+
- 13.9% — 11–15
- 41.3% — 6–10
- 37.6% — 1–5
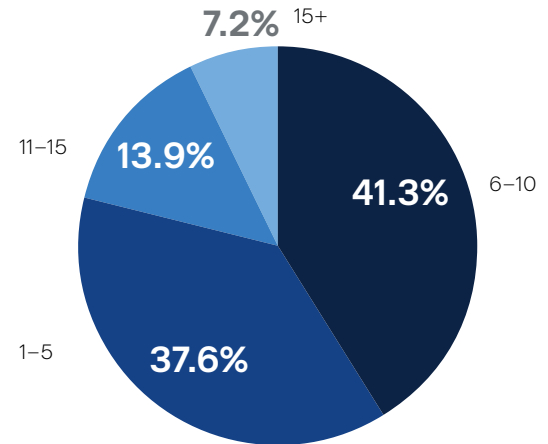
To defend against data loss and cyberthreats, IT professionals have stocked their IT stacks with all of the recommended cybersecurity technologies. Organizations have assembled highly complex patchworks of solutions – most relying on up to 10 different services and agents to defend their data, applications, and systems. Unfortunately, this patchwork defense doesn't work against modern IT challenges and the complexity introduces mistakes that can be costly.

Half of organizations suffered downtime, nonetheless

In the past year, has your organization experienced data loss that resulted in downtime?

Even with more IT professionals backing up and enabling more cybersecurity services within their environments, half of the IT professionals we surveyed reported data loss that resulted in downtime in the past year. Given how much time and money goes into maintaining and managing these solutions and how costly downtime can be for an organization, this is a serious issue that speaks to the ineffectiveness of this patchwork solution. Compared to last year, the number of organizations with data loss increased by 7%. Before that, it grew 11% year-over-year, indicating that the issue is getting worse.
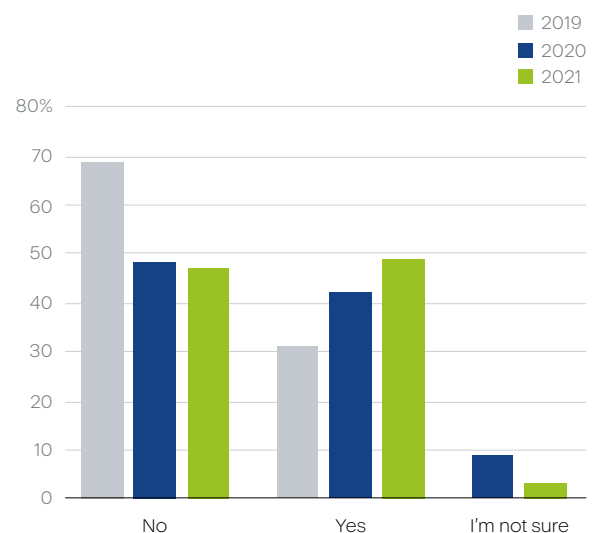
Remote work challenges persist for IT professionals

In the last year did your organization shift to increased remote working environments?
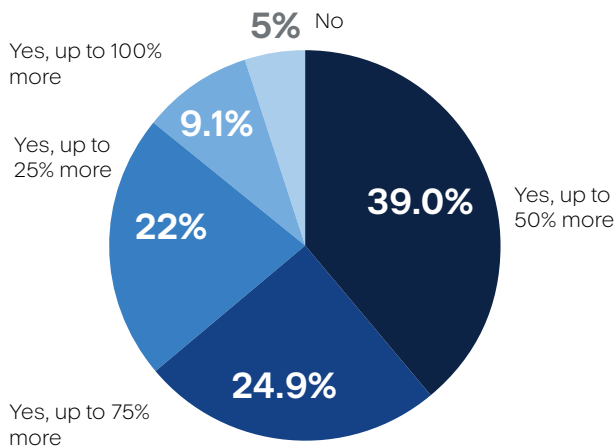
5% No

9.1% Yes, up to 100% more

Yes, up to 25% more

22%

39.0% Yes, up to 50% more

24.9%

Yes, up to 75% more

What has been the biggest IT challenge your organization faced during and following the shift to remote work?

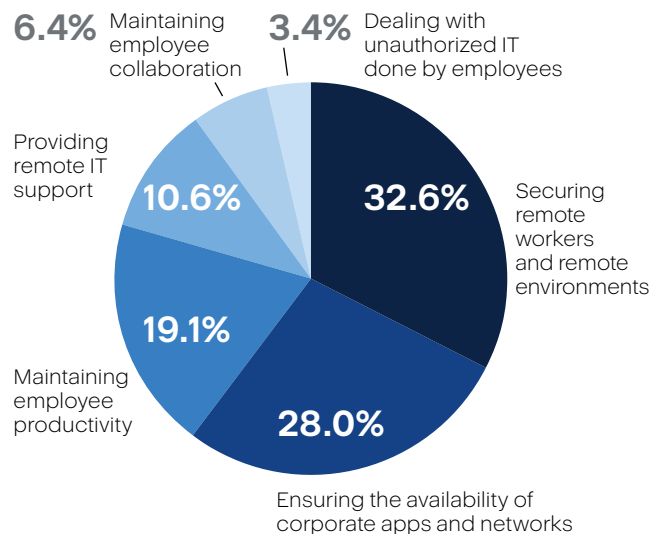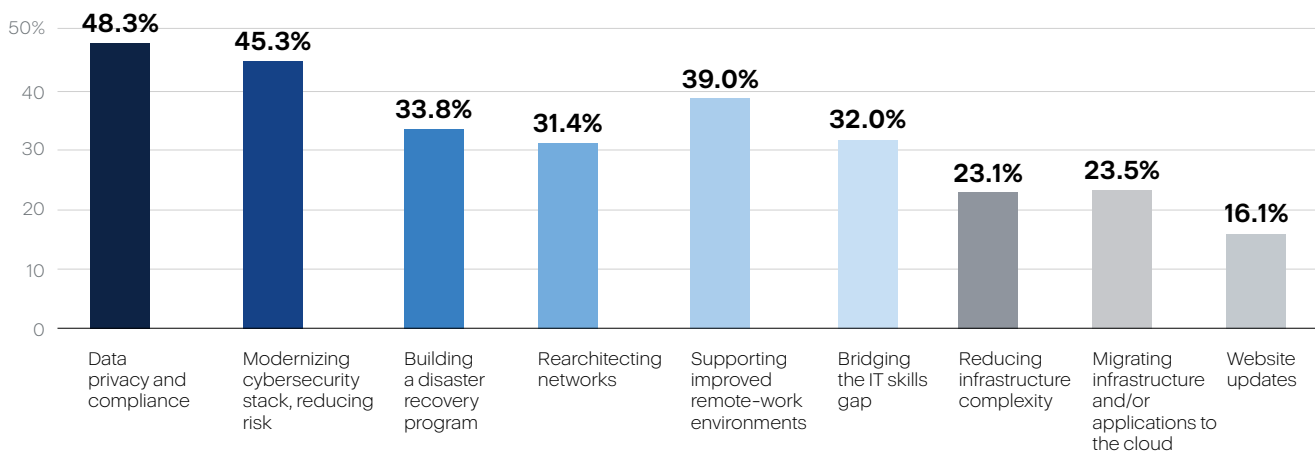**6.4%** Maintaining employee collaboration

3.4% Dealing with unauthorized IT done by employees

Providing remote IT support

10.6%

32.6% Securing remote workers and remote environments

19.1%

Maintaining employee productivity

28.0%

Ensuring the availability of corporate apps and networks

The drastic shift to remote work during the COVID pandemic saw 95% of organizations moving some portion of their staff away from offices and many of the challenges that arose during that move continue into 2021. As we shared in our 2020 Cyber Readiness Report, these top challenges included enabling/instructing employees on remote work, securing remote work, and ensuring the availability of corporate apps and networks – all of which remain significant challenges according to this new research.

IT priorities and spending in 2021

What IT projects are you prioritizing in the year ahead?

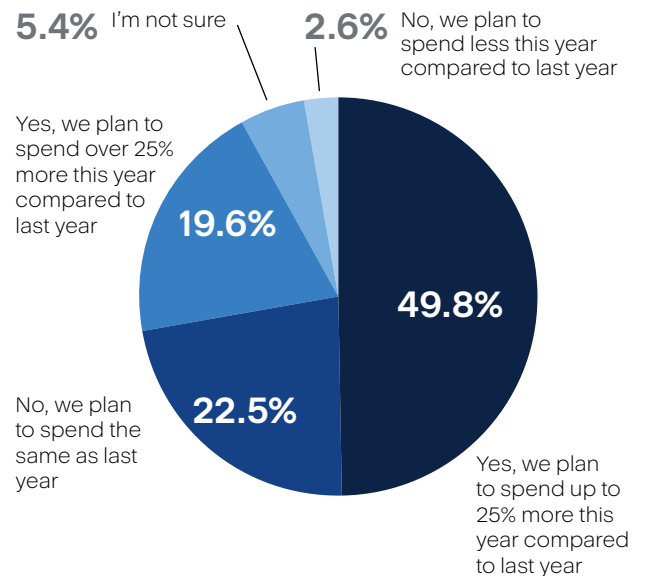| Category	Percentage
Data privacy and compliance	48.3%
Modernizing cybersecurity stack, reducing risk	45.3%
Building a disaster recovery program	33.8%
Rearchitecting networks	31.4%
Supporting improved remote-work environments	39.0%
Bridging the IT skills gap	32.0%
Reducing infrastructure complexity	23.1%
Migrating infrastructure and/or applications to the cloud	23.5%
Website updates	16.1%

Is your company planning to spend more to meet those IT challenges in 2021?

These challenges and experiences in mind, IT professionals are pursuing a wide variety of IT improvements and enhancements in the year ahead. Top priorities include enhancing data privacy and compliance processes, modernizing cybersecurity to reduce risk, and supporting remote work environments into 2021. It's worth noting that privacy and compliance earning the top prioritization spot is interesting given that nearly a quarter of organizations claim they aren't (or aren't aware) of data privacy requirements that affect them.

Frustratingly, a much smaller segment is prioritizing the reduction of infrastructure complexity, which could have an instant positive effect on many of the challenges that IT teams now face – including the budget limitations that a patchwork of IT solutions creates.

That said, 70% of organizations are planning to increase their 2021 IT budget compared to last year. This suggests that IT professionals are

mindful of the challenges their organizations are facing and are prepared to find modern solutions to address them, upgrading outdated and ineffective solutions with modern solutions that better address today's IT challenges.

5.4% I'm not sure

2.6% No, we plan to spend less this year compared to last year

Yes, we plan to spend over 25% more this year compared to last year

19.6%

49.8%

No, we plan to spend the same as last year

22.5%

Yes, we plan to spend up to 25% more this year compared to last year

Conclusion

KEY TAKEAWAYS

The solutions and approaches that personal IT users and professional IT teams have relied on for years are no longer enough to ensure data protection and cybersecurity. Our research finds that a rethought approach is essential to achieving a more reliable, holistic defense for the data, applications, and systems, particularly one that

Simplifies cyber protection

Connects disparate capabilities

Informs users about the status of their defenses

Reduces complexity

Acronis Cyber Protection Solutions deliver all of these benefits, unifying modern data protection, cybersecurity, and endpoint management capabilities into a single platform, console, and user experience.

Empowering service providers

Acronis has long recognized the cost, efficiency, and security challenges that arise from using multiple solutions, which is why the company pioneered the field of cyber protection, integrating cutting-edge cybersecurity, best-of-breed backup, and endpoint management in a single solution.

For managed service providers, Acronis Cyber Protect Cloud is a single solution installed with one agent and managed through one console that delivers a set of essential cyber protection capabilities included a no cost or on a pay-as-you-go basis, enabling MSPs to build services at little to no upfront cost. Additional protection packs of Advanced Backup, Advanced Security, Advanced Disaster Recovery, and Advanced Management give MSPs the flexibility to further expand their services based on client needs.

GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

SECURITY
- #CyberFit Score
- Vulnerability assessment
- Active protection
- Antivirus and anti-malware protection without local signature-based detection
- Device control

NOTARY (PAY-AS-YOU-GO)

MANAGEMENT
- Group management of workloads
- Centralized plans management
- Remote desktop
- Remote assistance
- Hardware inventory

A

Workload

BACKUP (PAY-AS-YOU-GO)
- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY
- Test failover
- Cloud-only VPN connection

FILE SYNC AND SHARE (PAY-AS-YOU-GO)

The centralized management ensures MSPs can ensure their clients are fully protected without having to juggle multiple solutions. A single pane of glass provides the visibility and control needed to deliver comprehensive cyber protection - from creating local and cloud-based backups to stopping zero-day malware attacks with an advanced AI-based anti-malware and antivirus defenses that are VB100 certified.

Learn more and start building your services here:

LEARN MORE

Acronis

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. With award-winning AI-based anti-malware 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 1,500 employees in 33 locations in 18 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages. For more information, visit www.acronis.com