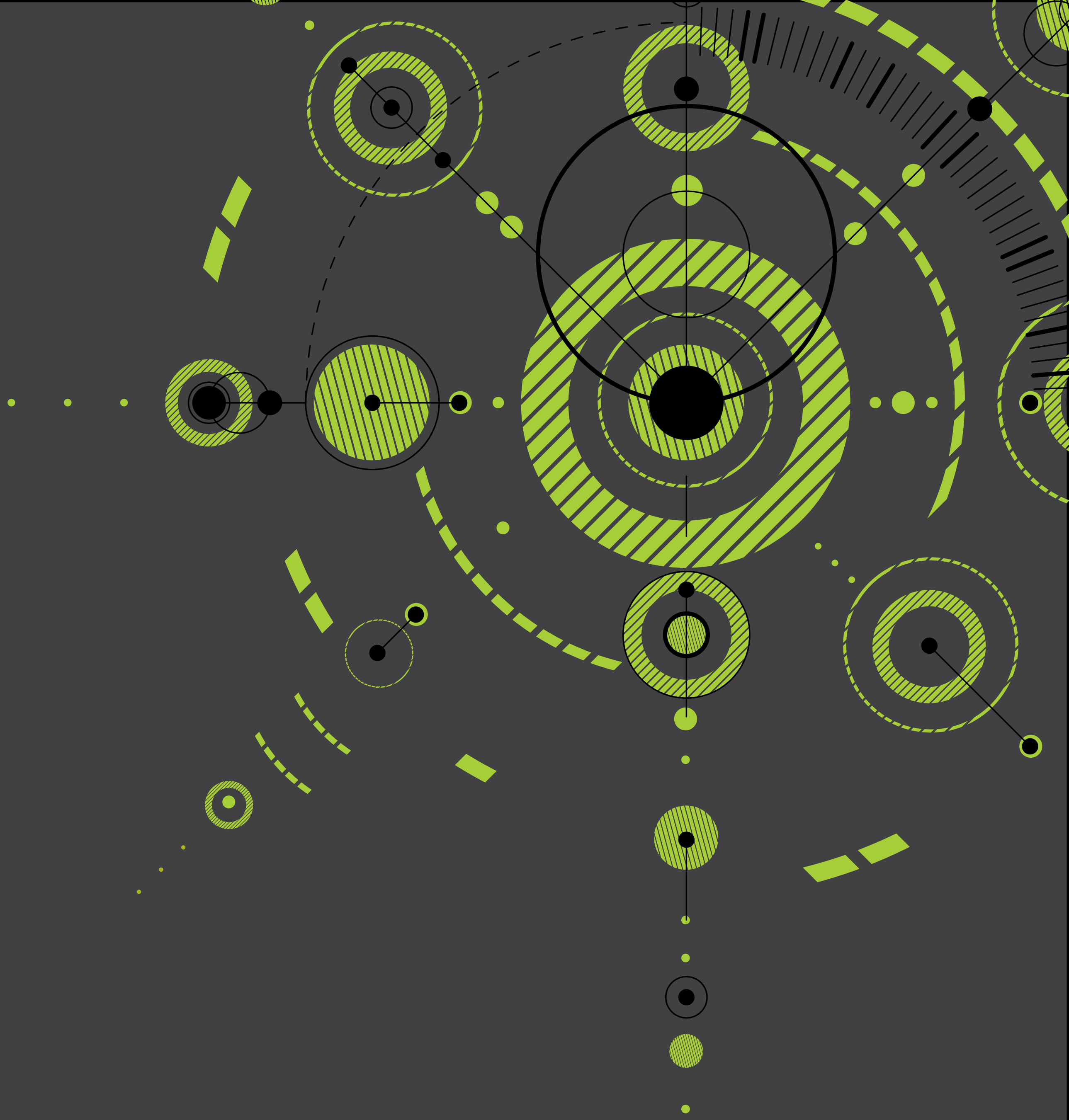
Quorum’s State of Disaster Recovery Report 2016



If Ben Franklin were alive today, he'd probably say that there were only three things certain in life: death, taxes and IT disasters.

Every organization has had their share of trouble, whether a flood, a hardware failure or an overseas criminal. Yet as the demand for 24/7 uptime grows more urgent, and new cloud solutions transform the world of backup and disaster recovery, many teams are struggling to understand the tools and strategies required for a successful BDR program.

We asked top IT professionals 10 questions about their risks and challenges.

Some teams view DRaaS as a panacea that will eradicate all backup headaches. Others are doggedly sticking with legacy systems no matter how arduous the resulting backup process. Almost all of them are wondering how their competitors are handling BDR and if they're behind the curve or leading the pack.

To find out, we asked top IT professionals — CIOs, CTOs and IT leaders of large, small and mid-sized companies — 10 questions about their risks and challenges, and the solutions they've found. These leaders told us what keeps them up at night; they told us what they dislike about their current BDR solution and what they're trying to do better. But mostly they gave us an idea of where this industry is headed, next month, next year and into the future.

Here are the results – followed by our conclusions about the state of disaster recovery today and tomorrow.

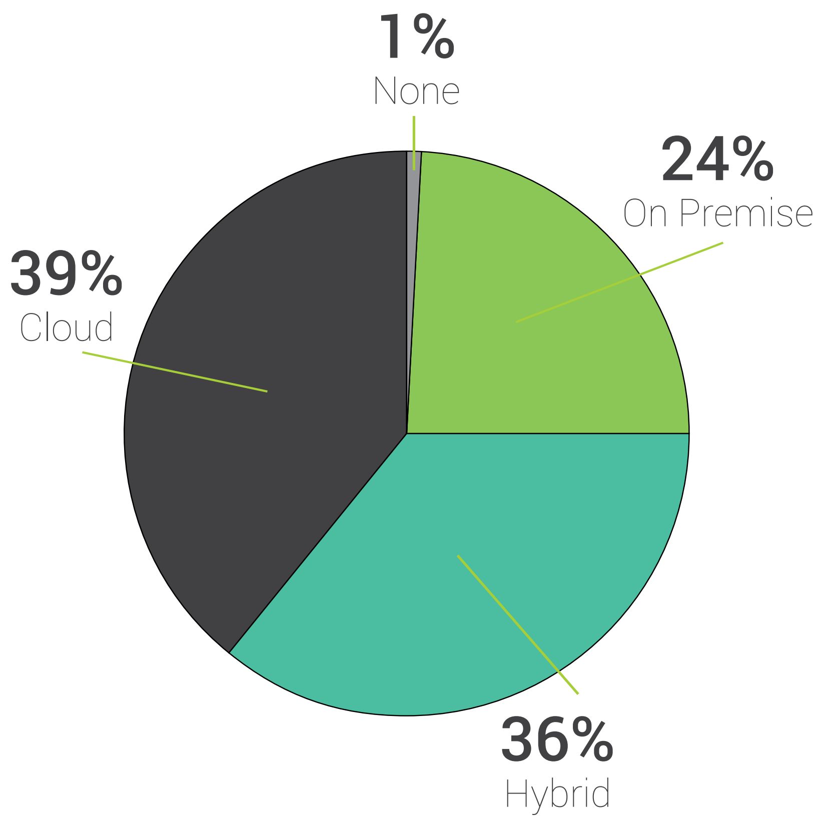
The Results

It’s a Recovery Revolution

1. What disaster recovery architecture are you currently using?

75% of respondents are using cloud-based disaster recovery solutions. 36% opt for a hybrid on premise and cloud model, and 39% use DraaS only.

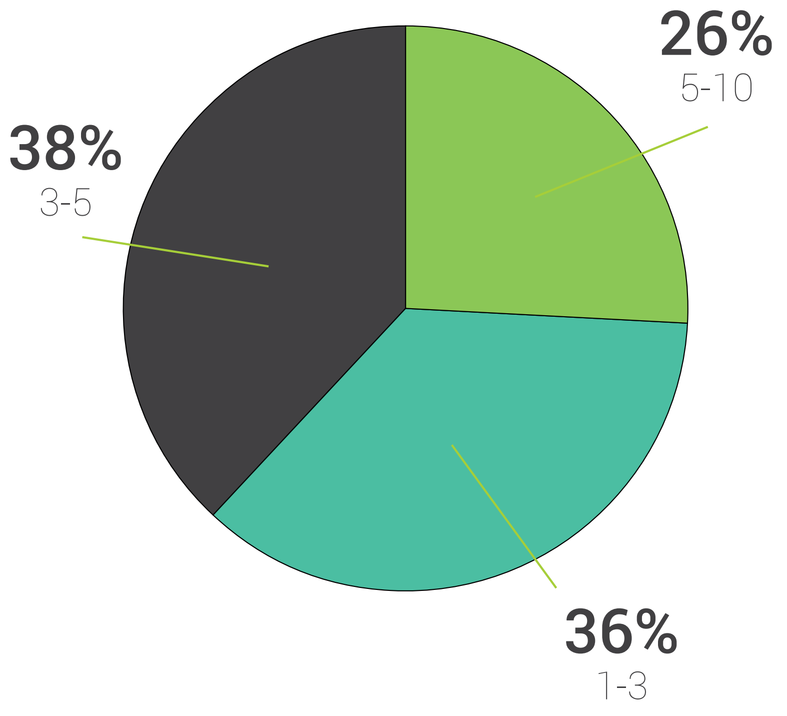
24% of respondents use only on premise disaster recovery solutions, rather than choosing the cloud.



2. How many backup and recovery products are you currently using?

64% of respondents are using more than 3 different disaster recovery solutions; 26% use over 5 different products.

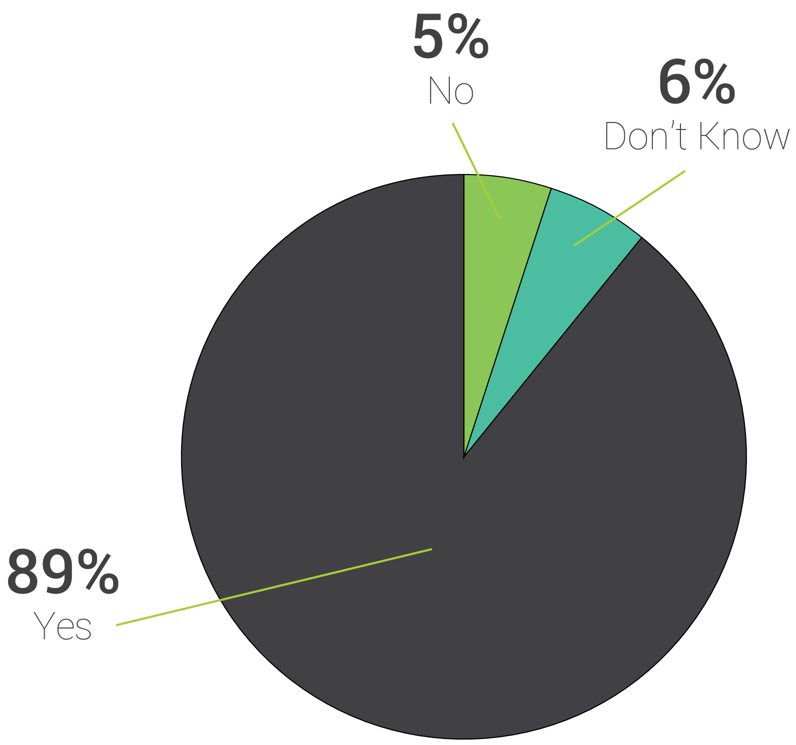
Less than 40% use between 1 and 3 different disaster recovery products with their organizations.



3. Are you planning or interested in implementing more cloud based disaster recovery?

89% see a future of more cloud-based disaster recovery.

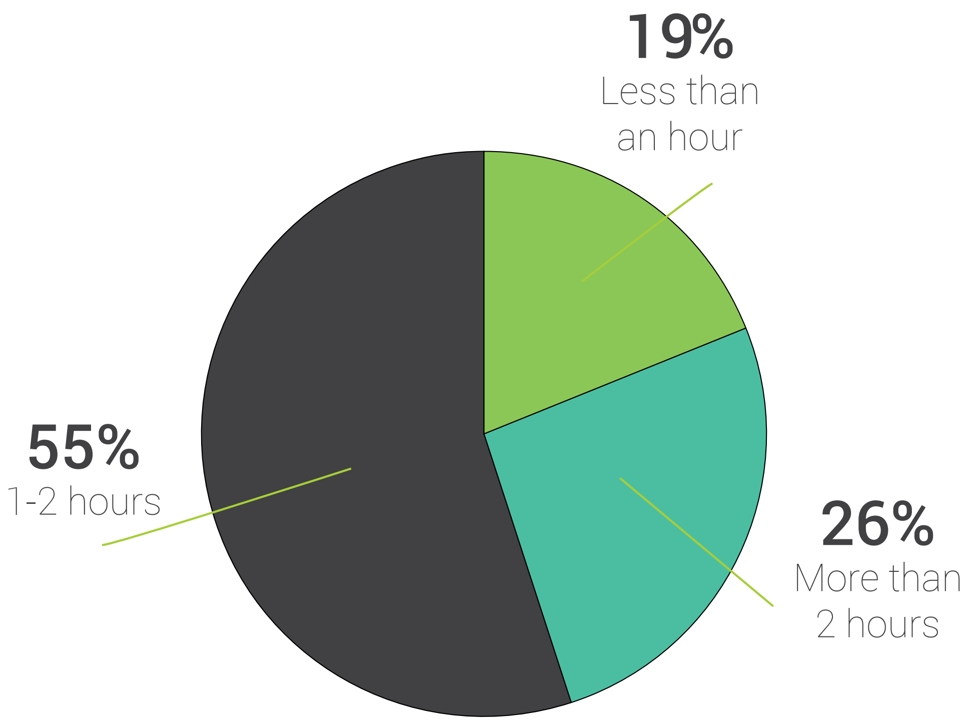
Less than 6% of respondents are interested in the same.



4. On average, how long will it take you to recover from a server failure?

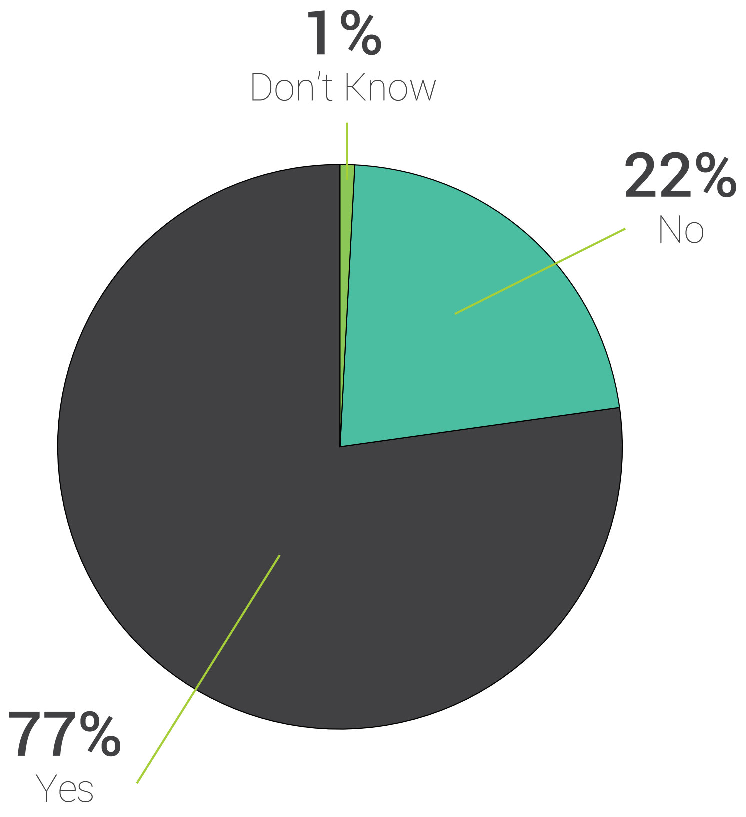
Over 80% of respondents say it takes more than an hour to recover from a server failure; more than a quarter say they need more than 2 hours.

Less than 20% claim they can recover from a server failure in under an hour.



5. Have you ever used your DR solutions after a security threat event, such as malware, or ransomware?

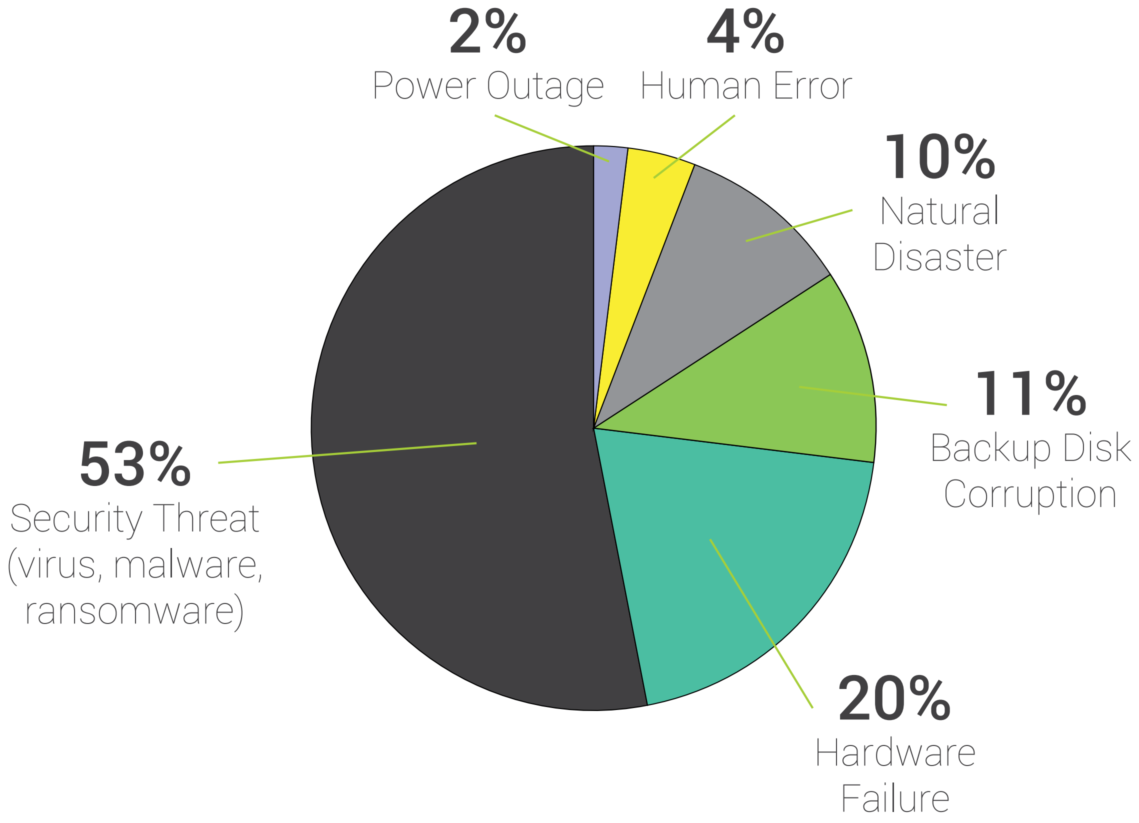
77% of respondents have used their disaster recovery solutions after a security threat event.



6. What are you most worried about?

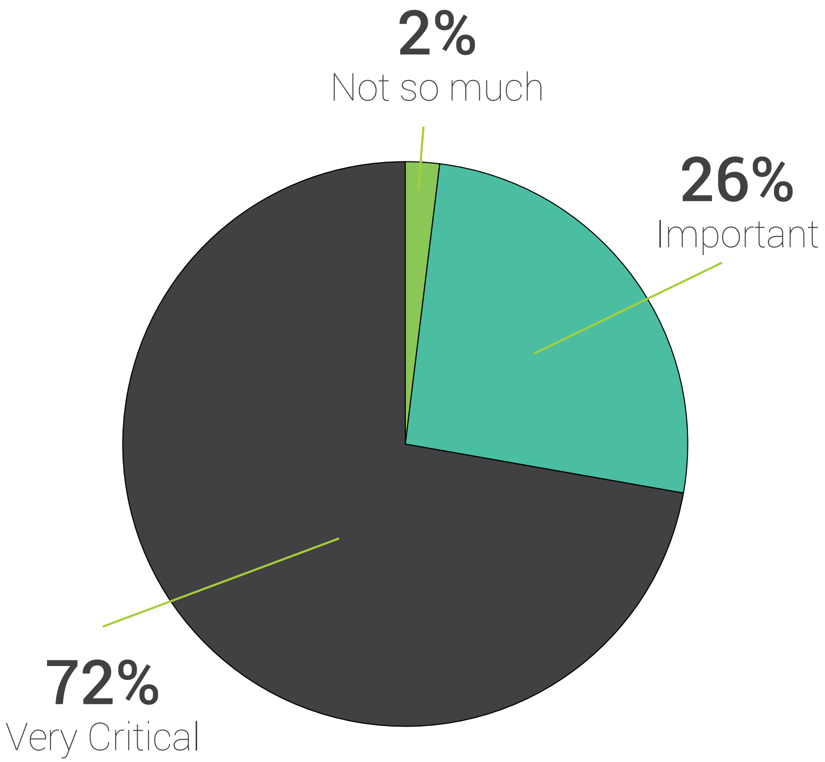
Over half of respondents are most worried about security threats compared to hardware failure or backup disk corruption.

47% are less concerned with a security threat than hardware failure, backup disk corruption or a natural disaster.



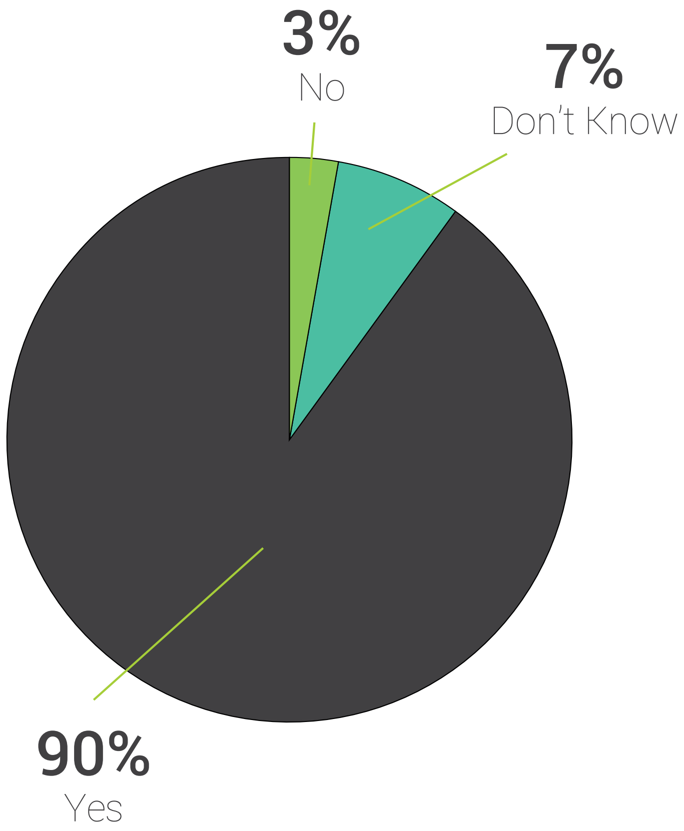
7. How critical is speed of backup and recovery of data for you?

98% believe speed of backup and recovery plays an important role, with 72% of them claiming it's very critical to their business.



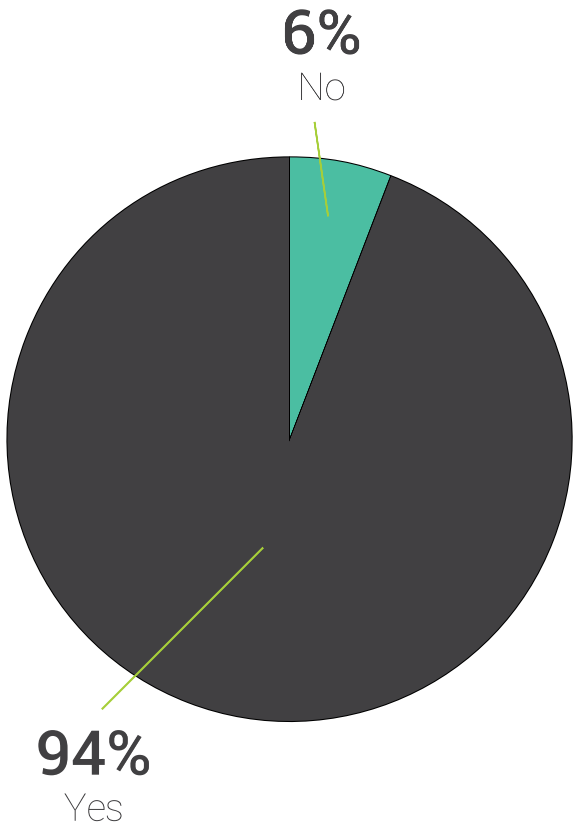
8. Would you be interested in consolidating your DR solutions into one dashboard?

90% of respondents would like to consolidate their disaster recovery solutions into one dashboard.



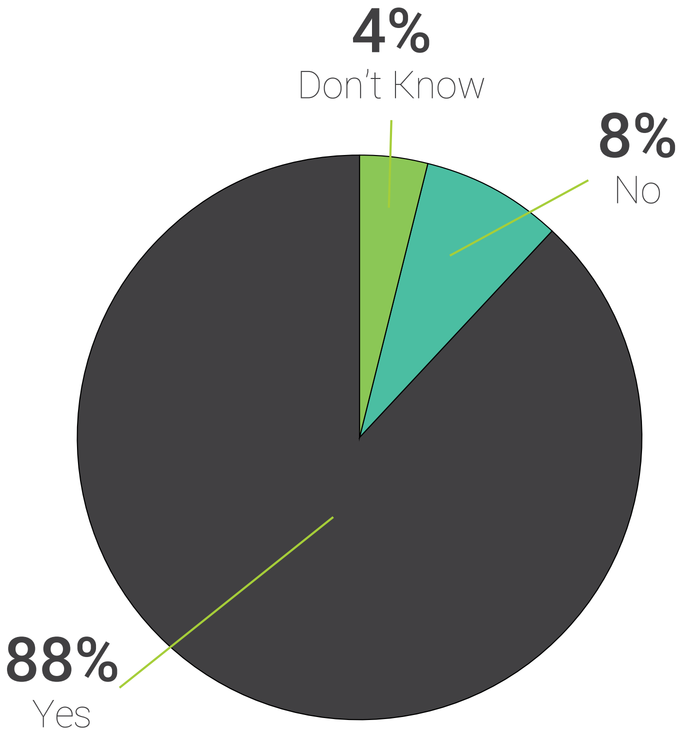
9. Do you regularly test your backups?

94% of respondents regularly test their backups.



10. Are you able to do production level testing with your current disaster recovery solutions?

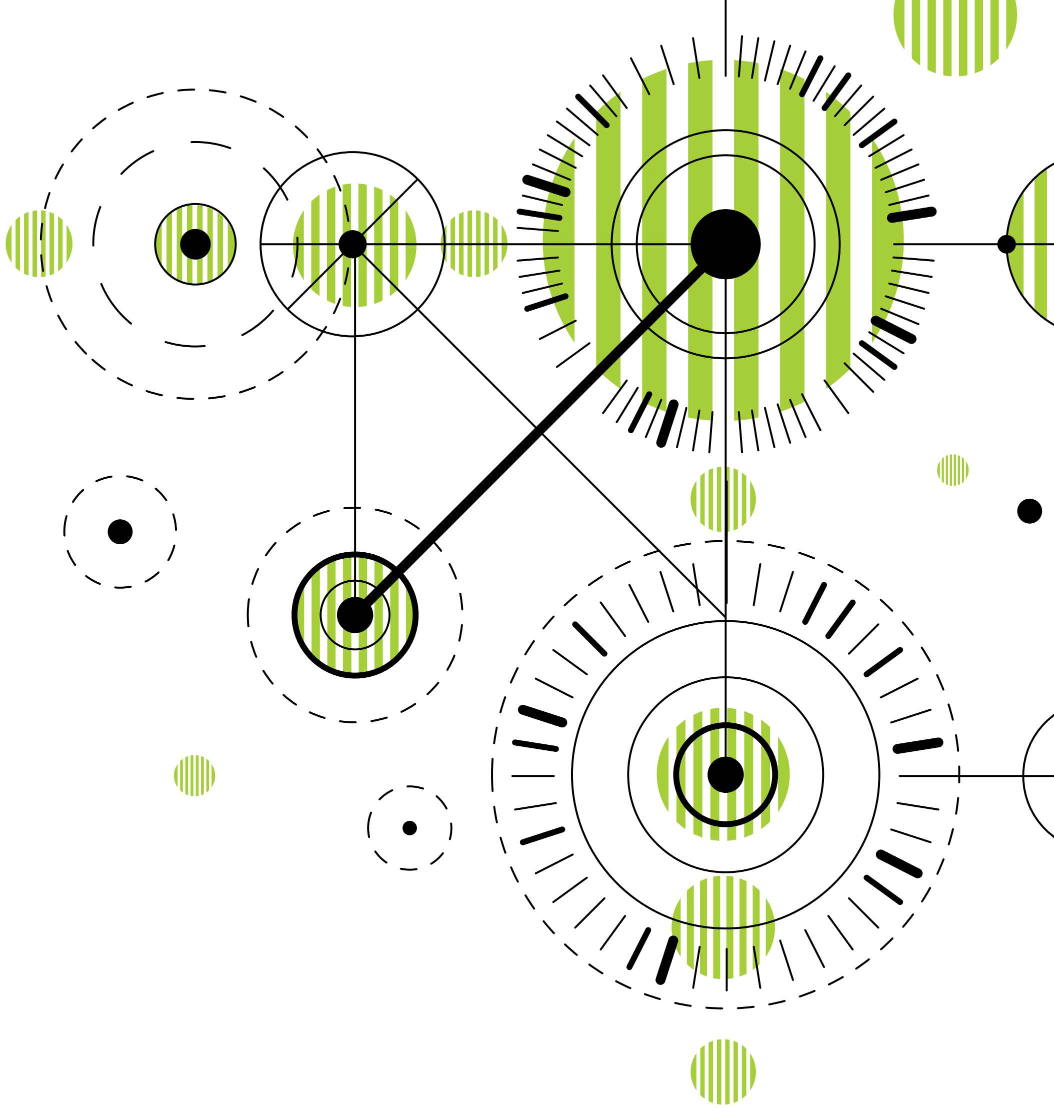
88% of respondents can achieve production level testing with their disaster recovery solutions.



What does it all mean?

Businesses of all sizes have their head in the cloud.

From the enterprise to the small business, 75% of teams recognize the cloud's ability to offer them offsite backups and stronger business continuity. A full 39% rely fully on the agility, security and cost savings of Disaster Recovery as a Service (DRaaS). Only 24% of respondents are using on premises disaster recovery solutions only – and it's a safe bet that many of them would like to change that, with 89% planning on implementing more cloud-based disaster recovery.



Teams are juggling way too many products.

64% of respondents are using more than 3 different disaster recovery solutions, with more than a quarter using over 5 different products. That's a lot of vendor management, a lot of money and – just a guess here – a lot of time spent getting these solutions to work together. Ideally teams should be getting their BDR needs met with just one or two products, but only 36% of respondents are. No doubt that's why so many crave simplicity: an astonishing 90% want to consolidate their disaster recovery solutions into one dashboard. But there's good news too, considering 88% can and do achieve production level testing using their BDR solution.

… And yet their recovery is way too slow.

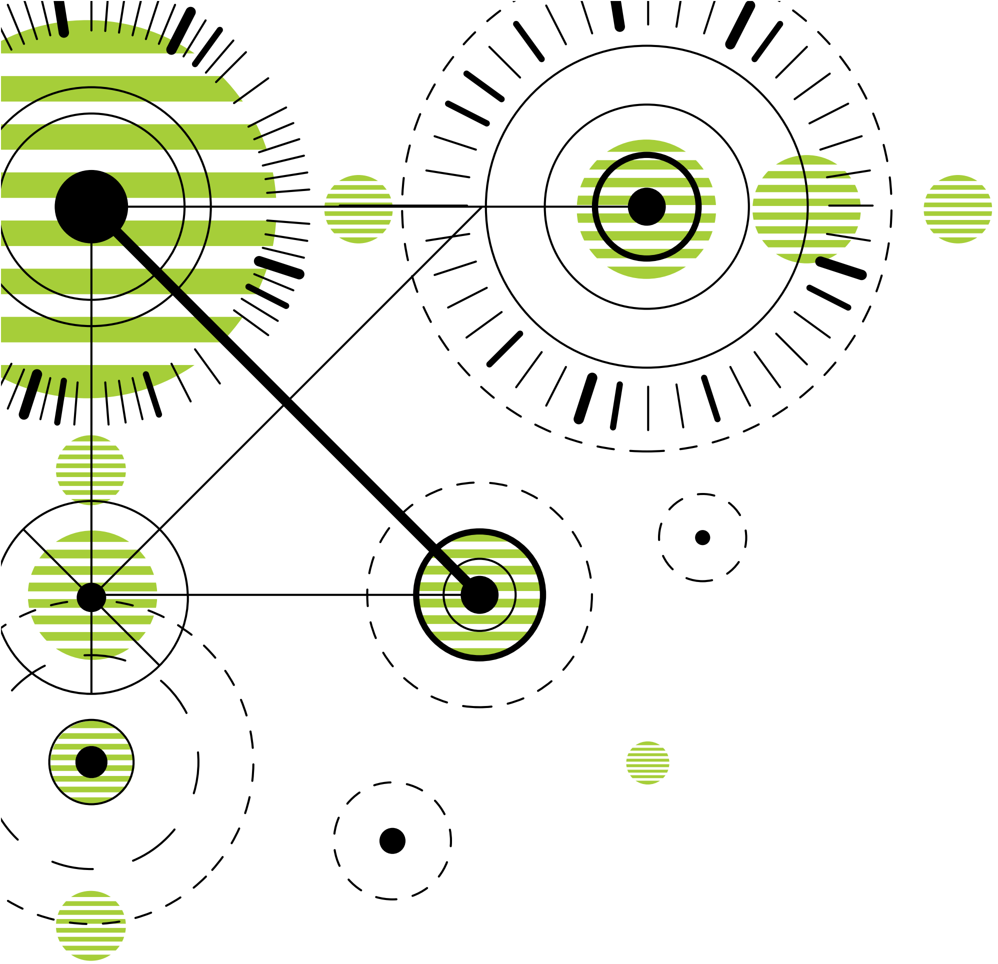
All those BDR products aren't making their recovery any faster. While speed is essential for continuity and security – not to mention brand reputation – a staggering 80% of respondents need more than an hour to recover from a server failure. And it gets worse: more than a quarter need more than 2 hours. Yet a full 98% of respondents realize their speed of backup and recovery is important, with 72% rating it as very critical to their business. There's a serious conflict here that's at the heart of BDR challenges today.

A cyberattack is an IT leader’s biggest fear.

Over half of respondents worry more about security threats than hardware failure or backup disk corruption. That’s hardly surprising, given the recovery delays above. Natural disasters crashing in on a data center, an employee error or a hardware failure can all pose immense problems for an organization. But a skilled and willful attack can cripple a brand for years and could cost a literal fortune. Ransomware attacks particularly depend on a team’s inability to recover quickly.

Disaster recovery is a critical security defense.

There might still be a few teams out there minimizing the importance of an advanced backup and data recovery solution, but most have learned otherwise the hard way. More than three quarters of respondents have used their disaster recovery solutions after a security threat event.



It's clear that changes in the world of BDR are highlighting old frustrations for some leaders even as they light the way to stronger and faster solutions for others. As more organizations explore cloud-based backup and recovery and virtual environments, they are finding ways to accelerate recovery while minimizing costs. It's clear the right strategies and solutions are available – and that IT leaders have their eyes on a future of faster recovery and stronger security.

Quorum®
1-Click Instant Recovery

www.quorum.com