UNITRENDS

PRIANTO
Knowledge Distribution

THE UNITRENDS STATE OF BCDR SURVEY REPORT 2021

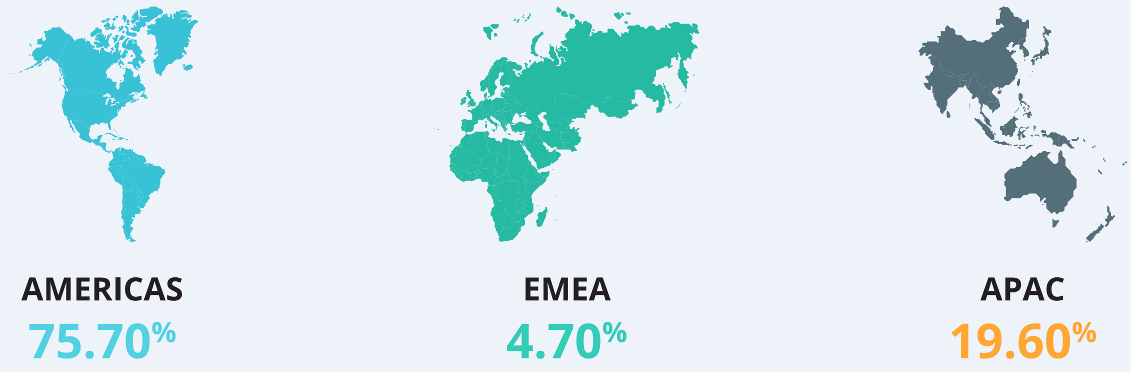
Introduction

Unitrends surveyed more than 750 IT professionals from organizations worldwide to learn about how their approaches to business continuity and disaster recovery (BCDR) are adapting to support today's hybrid workforces in a digital global economy. The result is a wealth of data and insight that range from how organizations are leveraging cloud-based technologies, combating sophisticated cyberattacks and what the BCDR "must-haves" are to keep pace with the rapid changes taking place.

Our research extends beyond Unitrends adopters and customers to gather insights beyond our user base while ensuring we have strong representation across industry verticals and organizations of varying size throughout the Americas, EMEA and Asia Pacific regions. We've included a Table of Figures at the end of our report, which breaks down representation by region, vertical and industry.

For the purpose of reporting our findings, we have aggregated much of our data by organization size, categorizing respondents as representatives of Small to Midsize "SMB" (<500 employees) and Mid-Market to Enterprise "MME" (>500 employees) organizations. Respondents from SMB organizations represent 52.34% of our survey data and MME organizations 47.66%. See Figures 1 and 2 in the appendix for a breakdown of responding organization by employee size and industry vertical, respectively.

Respondents from SMB organizations represent 52.34% of our survey data and MME organizations 47.66%.



RESPONDENTS BY REGION

Key Findings

1. Cybersecurity and cyber resilience emerged as major priorities across the board

With the damages from cybercrime expected to reach $6 trillion this year, cybersecurity and cyber resilience emerged as major priorities among both SMB and MME organizations with regards to their BCDR posture.[1] Organizations are looking to leverage automation, artificial intelligence and proactive monitoring to help combat the proliferation of phishing, account takeover attacks (ATO), ransomware and more.

2. A large portion of workloads will be delivered via cloud

Cloud technologies are increasingly popular in both production and BCDR use cases. Global cloud spending is expected to exceed $332 billion in 2021 — a 23% increase from 2020's $270 billion spend.[1] Beyond traditional use cases, such as archiving and failover, both SMB and MME respondents indicated increasing the number of workloads that are delivered via cloud versus on-premises infrastructure.

3. IT budgets will get bigger in 2022

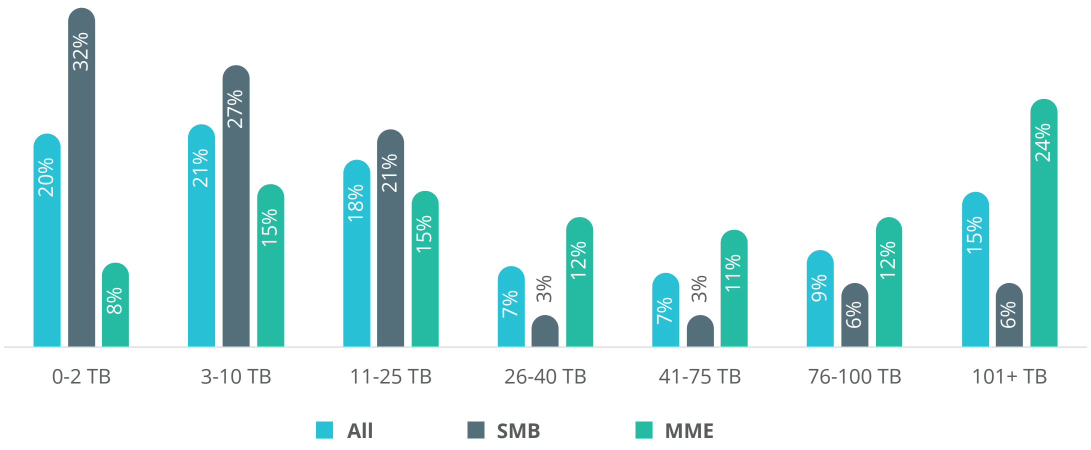
As we emerge from the depths of 2020's pandemic lockdown, the global economy is projected to grow 4.9% in 2022 thanks in part to governmental financial support and improving health metrics in the second half of 2021.[2] For many organizations, this return to growth is reflected in their IT budgets — more than one-third of respondents anticipate budgets will increase in 2022 while another third anticipate flat budgets. Less than one in ten respondents anticipate IT budget cuts.

The State of Protected Environments

We found some correlation between employee size and the volume of protected data among our respondents, with MME organizations reporting they work with significantly larger data volumes much more frequently.

About 36.71% of MMEs are backing up more than 75 TB of data compared to 12.42% of SMBs. Conversely, 60.25% of SMBs report backing up 10 TB of data or less. MMEs represented those protecting mid-to-large sized data sets (11-74 TB), 43% more frequently than SMBs (39.24% to 27.35%).

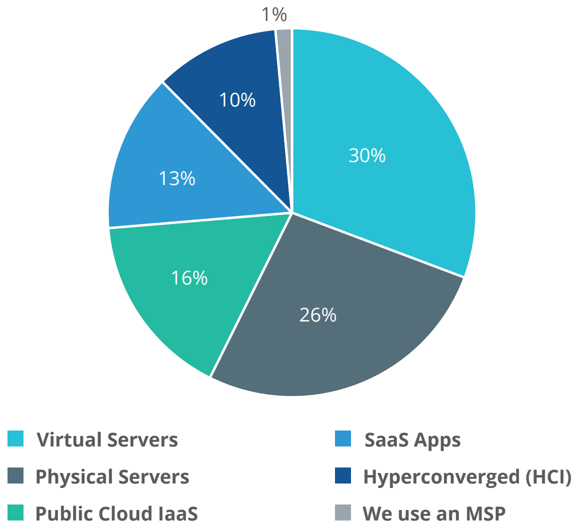
[HOW MUCH DATA ARE YOU BACKING UP TODAY?]



The majority of protected workloads are still being run on-premise currently. About 13% of all organizations polled cited all workloads are run exclusively from an on-premise environment. A large minority of both SMBs (46.28%) and MMEs (39.2%) reported at least three-quarters (75% or more) of their workloads are delivered by on-premise infrastructure.

Data protection for on-premise assets requires support for heterogenous environments. Respondents still rely heavily on physical servers (44.93%) and virtual severs (39.13%). While in many cases hyperconverged infrastructure (HCI), such as Nutanix or Scale Computing, runs virtual machines that can be protected at a hypervisor level, 15.94% of respondents have ditched the historically siloed approach to on-prem infrastructure to embrace HCI.

[WHICH OF THE FOLLOWING MOST CLOSELY DESCRIBES YOUR IT STACK?]



While on-prem assets accounts for the lion's share of respondents' protected environments, approximately 30% of workloads today are being delivered via cloud. Public cloud Infrastructure-as-a-Service (IaaS) accounted for 16% of all protected assets while SaaS applications make up another 14%.

In light of IaaS and SaaS data representing the smallest percentages of protected data, it's important to remember that SaaS providers such as Microsoft and their Microsoft 365 service operate under a **shared responsibility model**. Under this model, Microsoft SLAs do not provide customers protection against some of the most **common causes of SaaS data loss**. While their data centers are equipped with world-class disaster recovery capabilities to safeguard infrastructure and provide high availability, they cannot protect organizations' data from human error, business email compromise, ATO and other social engineering attacks.

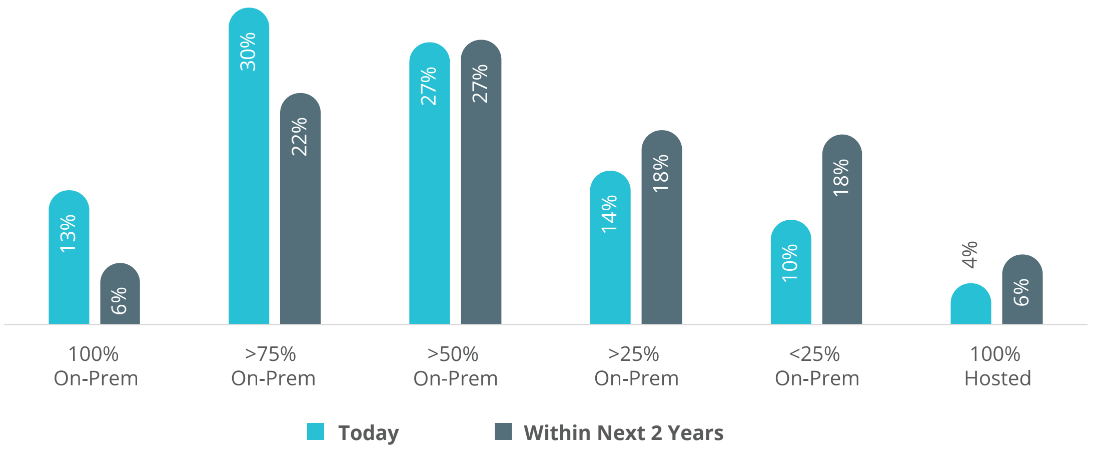
Forecasting Technology Trends

The agility, flexibility and scalability of the cloud has made it a popular choice for many organizations transitioning towards support of hybrid models. Reducing the on-premise infrastructure footprint appears to be a popular sentiment — is the percentage of all organizations that operate 100% cloud-hosted workloads is expected to increase by 70% over the next two years.

Overall, our respondents expect this trend to continue over the next two years, with 44% of respondents reporting they expect as many as half of all workloads to be cloud hosted compared to the current 29.1%.

Of the 29.1% of organizations that host at least half of their workloads in the cloud currently, 53% reported workloads categorized as public cloud Infrastructure-as-a-Service (IaaS) and 47% categorized as SaaS applications.

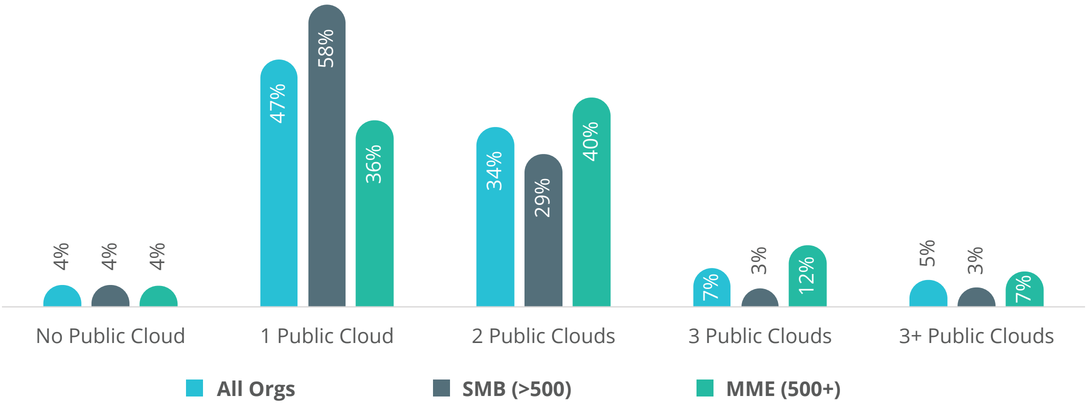
[IN THE NEXT 24 MONTHS, WHAT PERCENTAGE OF DATA DO YOU ANTICIPATE HOSTING ON-PREM VS IN-CLOUD?]



SMBs and MMEs project to adopt hosted technology at a similar rate. Of the organizations reporting all workloads hosted on-premise currently, 45.8% of SMBs and 46.4% of MMEs plan to migrate a portion of their applications and services to cloud-hosted platforms over the next two years.

The majority of MMEs spread workloads across several cloud providers — 40.62% utilize two distinct public clouds, 12.04% utilize three and 7% have workloads in more than three public clouds. By contrast, SMBs have adopted public clouds at a slower rate, with the majority (58.67%) reporting usage of one public cloud and 29.59% utilizing two public clouds. Only 7.4% SMBs utilize three or more public clouds.

[DOES YOUR ORGANIZATION CURRENTLY USE OF ONE OR MORE PUBLIC CLOUD PLATFORMS?]



Cloud adoption is a trend we may see continue, especially as many anticipate their IT budgets will increase next year. About 37.53% of SMBs and 36.72% of MMEs reported they expect IT budgets to increase. Less than 10% of SMBs (9.32%) and MMEs (7.76%) anticipate budgets will decrease. Nearly 37.26% of SMBs and 38.21% of MMEs expect budgets to remain flat, while the remainder reported being unsure. See Figure 6 in the Appendix for all budget predictions.

The Cloud's Use in BCDR

Beyond hosting production workloads, respondents identified the cloud as a key aspect of their overall BCDR strategy. A small minority of SMBs (10.62%) and MMEs (8.78%) reported not using the cloud as part of their BCDR strategy.

The three most commonly cited use cases for the cloud in BCDR are:

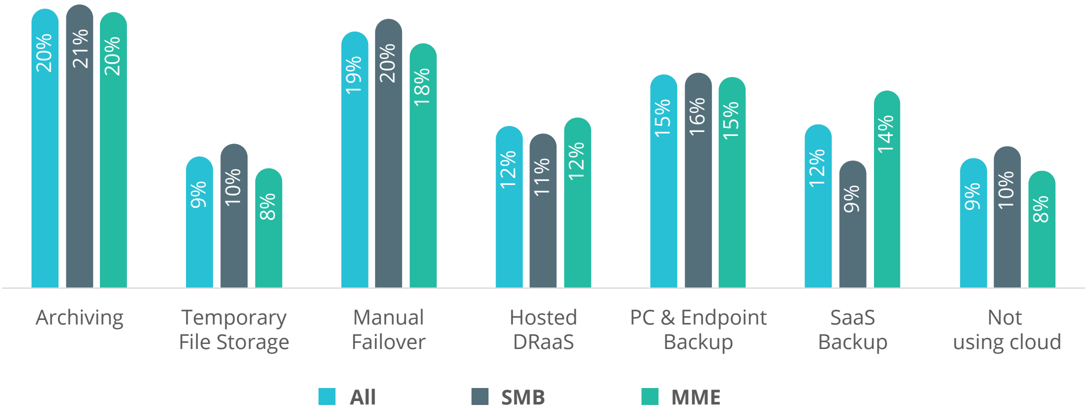
1. Archiving/Long-Term Retention (21.24% SMB, 20.64% MME)
2. Manual Failover/Disaster Recovery (20.18% SMB, 18.30% MME)
3. Backup for PCs & Endpoints (16.08% SMB, 15.81% MME)

Since the start of the COVID-19 pandemic, 16% of companies have gone fully remote and 62% of workers claim to work from home at least "occasionally."[3] With critical data and IP being created on remote devices, endpoints and on remote networks, it's critical to back up user data to maximize productivity and protect your businesses' digital intellectual property.

IT professionals that work with a traditional data protection infrastructure may struggle to protect data on remote endpoints. A staggering 98% of stolen laptops are never recovered, making endpoints one of the weakest links of the security environment and bringing about the rising importance of **endpoint backup** in modern-day data protection.[5]

We were surprised to find SMBs report adopting hosted Disaster-Recovery-as-a-Service (DRaaS) at a similar rate as MMEs. Typically, MMEs have larger IT teams to support more specialization and diverse skill sets. Perhaps the cloud serves as an equalizer for SMBs, offsetting the cost and overhead of maintaining a secondary DR site with limited staff and smaller overall budgets. **DRaaS** enables businesses to leverage the experience of cloud providers to perform the heavy lifting with regards to implementation, failover and recovery of service, thereby reducing the burden on IT admins and freeing up their time to pursue more strategic initiatives.

[HOW ARE YOU USING CLOUD AS PART OF YOUR BCDR FUNCTIONS? SELECT ALL THAT APPLY.]



The three least commonly cited use cases for the cloud in BCDR are:

1. Short-Term File Storage (10.77% SMB, 8.93% MME)
2. Hosted DRaaS (11.53% SMB, 12.74% MME)
3. SaaS Backup and Recovery (9.56% SMB, 14.79% MME)

The limited use of SaaS Backup and Recovery solutions by SMBs may in part be due to the slower rate of cloud adoption. MMEs cited "Protecting SaaS application data" as a top data protection priority 46% more frequently than SMBs.

72.34% of SMBs said that most workloads (50% or more) exist on-premises currently. Approximately 18.62% of SMBs reported their workloads are entirely on-premise while another 27.66% of SMBs are more than 75% on-premise today. By comparison, only 7.49% of MMEs cited being entirely on-premise while 60.81% of MMEs cited at least a 50/50 split between on-prem and cloud workloads.

Top BCDR Trends

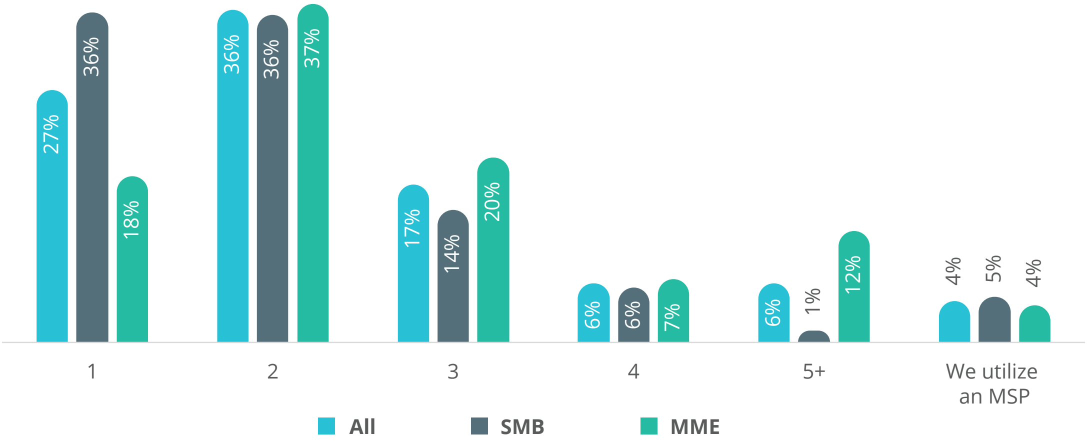
Slower rates of adoption and/or the lack of diversity in cloud platforms may also influence the number of unique backup and disaster recovery solutions utilized by organizations today.

36.53% of SMBs cite using only one unique vendor for BCDR compared to only 18.48% of MMEs.

Nearly twice the number of MMEs are utilizing three or more unique vendors for backup and disaster recovery compared to SMBs (39.89% to 22.13%). As workloads diversify, many organizations are left scrambling to fill in gaps that legacy providers cannot protect.

In part, the problem is the fallacy of "more is better," resulting in significant investments made across multiple vendors to protect an increasingly diverse set of platforms. This so-called "modernization" leaves IT pros with a complicated BCDR infrastructure that results in decreasing productivity, increasing errors and expensive overheads with few tangible benefits.

[HOW MANY UNIQUE SOLUTIONS ARE YOU USING FOR BACKUP AND DISASTER RECOVERY?]



The number of unique point products corresponds with the time invested in managing these solutions. MMEs revealed they are investing significantly more time (across all staff) managing BCDR solutions today compared to SMBs.

- More than a quarter of all MMEs (25.59%) report spending 25+ hours weekly managing BCDR (compared to just 5.88% of SMBs).
- The majority of SMBs (62.83%) report spending five hours per week or less managing BCDR (compared to 28.82% of MMEs).

See Figure 4 in the appendix for the full results.

On a related note, MMEs cited "Management of Multiple Solutions" as their top BCDR-related challenge 32% more than SMBs. Instead of a piecemeal approach to BCDR, as environments change, businesses should look to adopt a **unified approach to BCDR** — one with the flexibility and agility to adapt to environmental changes in both the short and long term.

Unification of BCDR components, in part achieved by injecting automation and artificial intelligence to streamline workflows and simplify complex systems, may help alleviate personnel-related struggles.

The complexity and cost of operating multiple, disparate solutions may prove prohibitive for smaller organizations who attempt to keep pace in the market today. SMBs cited "Increasing IT Costs" as their top-BCDR related challenge 19% more frequently than MMEs.

However, challenges relating to personnel (including bandwidth of staff, hiring challenges and internal knowledge gaps) were cited at similar rates among SMBs and MMEs

Top BCDR-related challenges:

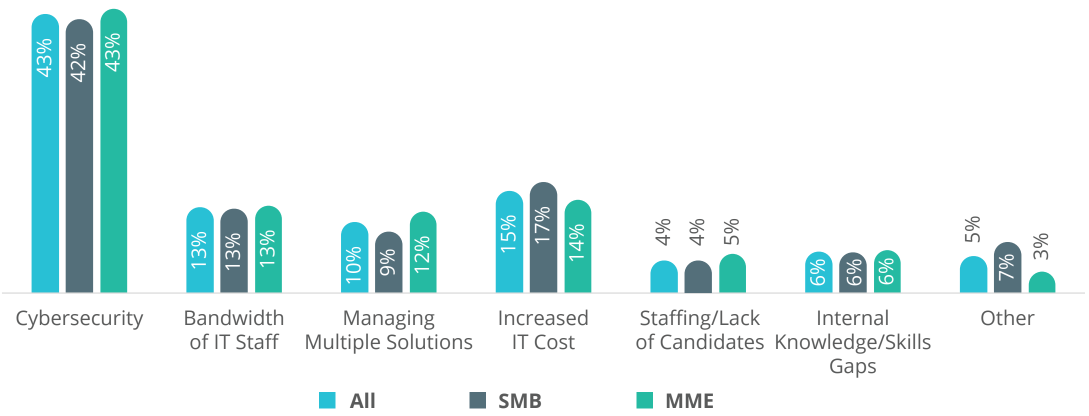
- Bandwidth of IT Staff (13.01% of SMBs, 13.43% of MMEs)
- Internal Knowledge/Skill Gap (6.23% of SMBs, 6.57% of MMEs)
- Hiring/Lack of Quality Candidates (4.07% of SMBs, 5.97% of MMEs)

As such, it isn't surprising to find ease of use and automation among the top three ranked attributes of respondents' "ideal" BCDR solution, with average scores of 4.24 and 4.18 respectively. We asked our respondents to rank a series of characteristics on a 1-to-5 scale, with 5 indicating the "most important."

Cybersecurity

Given the landscape of today's advanced cyberthreats, it's no surprise to see cybersecurity as a top concern for organizations of all sizes.

[WHICH OF THE FOLLOWING BCDR CHALLENGES IS MOST RELEVANT TO YOUR ORGANIZATION?]

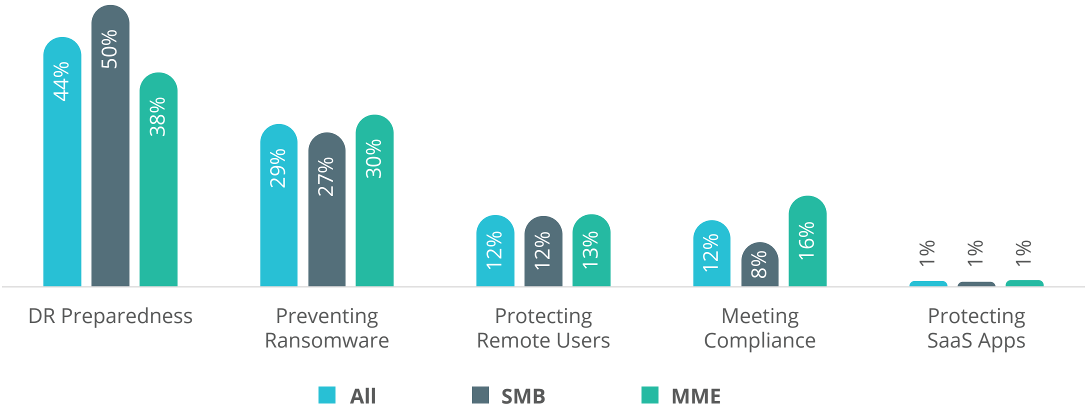


Cybersecurity was far and away the most frequently cited BCDR-related challenge, with 43.04% of all organizations indicating cybersecurity as the challenge most relevant to their organization.

The identification of cybersecurity as a top challenge corresponds with organizations citing preventing attacks as one of their chief data protection priorities. About 30.91% of MMEs and 27.70% of SMBs identified preventing ransomware as their top data protection priority.

Similarly, organizations seem to understand the risks and threat vectors opened by a hybrid/remote workforce — 12.74% of SMBs and 13.03% of MMEs cited protecting remote users as their top priority today.

[WHAT IS YOUR TOP DATA PROTECTION PRIORITY?]



Organizations are employing a multi-faceted strategy to protect their users, data and digital assets from cyberattacks. See Figure 5 in the Appendix for the full set of responses.

With regards to protecting their environments against cyberattacks, organizations most frequently cited the creation of backup copies taken off network and secured at an alternate physical location as the most viable protection method.

About 32.37% of all respondents (and we'd argue everyone should be doing this in some capacity) are getting data off-site. Perhaps unsurprisingly, given some of the resistance to the cloud discussed earlier, respondents still identified removeable media (e.g., HDDs, LTO tapes) as the dominant strategy (21.69%), outpacing the use of immutable cloud storage (10.58%) at a nearly 2:1 rate.

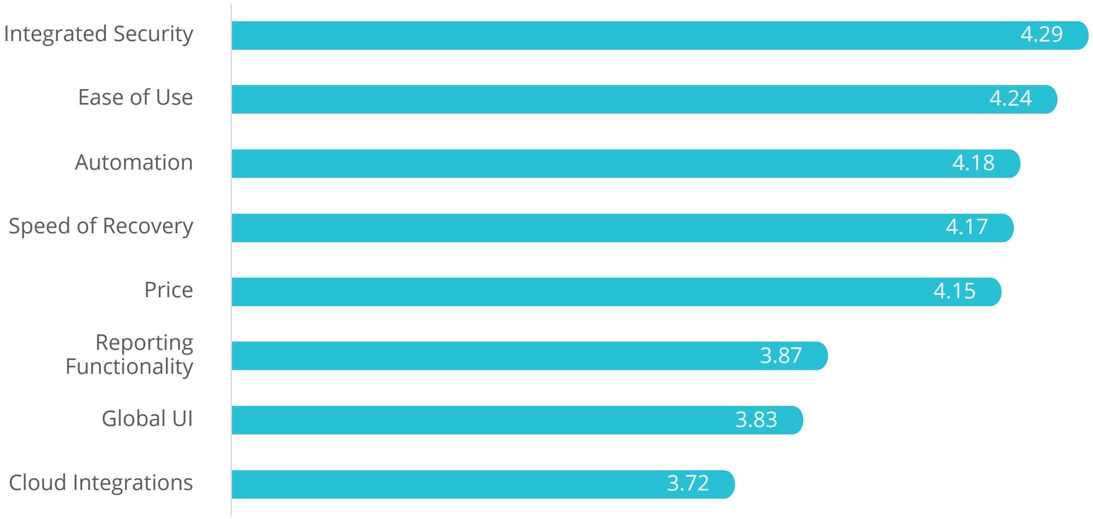
Immutable backups maintain an optimum number of recovery points and prevent any source from tampering with existing data storage blocks, resulting in an archive of backups that guarantee recovery by finding and restoring the last clean backup on record. Other strategies include proactive network monitoring (21.36%), end-user training and awareness (20.00%), and the utilization of a non-Windows-based backup solution (14.71%).

The greatest difference in strategies utilized came with automated DR testing. MME organizations reported automating their recovery testing 70% more frequently than SMBs. We cannot emphasize the testing aspect enough. **DR Testing** is integral to the success and resilience of a business in the face of disaster and is the surest way you'll know, with 100% confidence, that you can recover.

We asked respondents to rank a series of attributes on a 1 (least important) to 5 (most important) scale based on their ideal BCDR solution. Here, again, we saw an emphasis on security.

“Integrated Security” capabilities scored the highest, receiving 82.14% of 4- and 5-star ratings and the highest average score, 4.29. Cloud integrations (perhaps in part due to slower rates of adoption) scored as least important.

[RATE THE FOLLOWING ATTRIBUTES ON A 1-5 SCALE BASED ON YOUR “IDEAL” BCDR SOLUTION:]
(1 = LEAST IMPORTANT, 5 = MOST IMPORTANT)



Conclusion

More than two-thirds of both SMB and MME organizations anticipate IT budgets will grow or remain flat, further spurring cloud adoption to support a changing workforce and new delivery models. The number of organizations who host more than half of their workloads in the cloud is anticipated to increase by 51% over the next two years. As environments become more distributed and more complex, cybersecurity remains a priority, as does the ability to protect all these different sources of data with a solution that’s secure, easy to use and increasingly automated.

At Unitrends, our Unified BCDR platform enables our customers to address the challenges of today with a complete and agile solution designed to backup, secure and recover all workloads. The platform encompasses protection for traditional data center infrastructure as well as cloud-based workloads, SaaS data and the data being generated on endpoint devices such as small remote server, as well as laptops and remote PCs. Purposeful integrations with security tools provide end-to-end protection against cybercrime and human error, inject automation and artificial intelligence to simplify complex systems, and provide a unified experience with visibility across a complete backup infrastructure.

Appendix/Table of Figures

FIGURE 1

[RESPONDENTS BY EMPLOYEE SIZE]

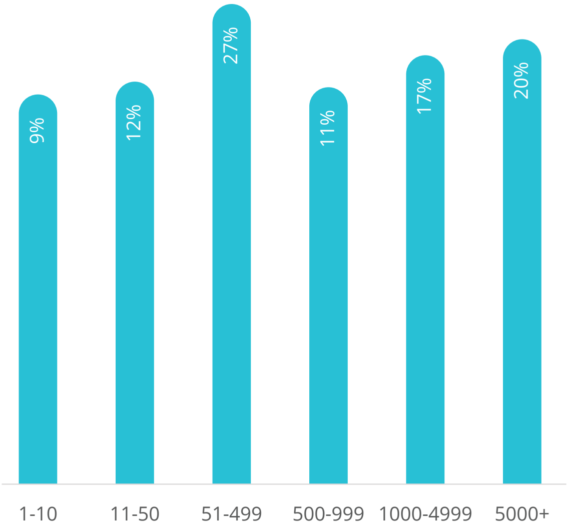


FIGURE 2

[RESPONDENTS BY INDUSTRY VERTICAL]

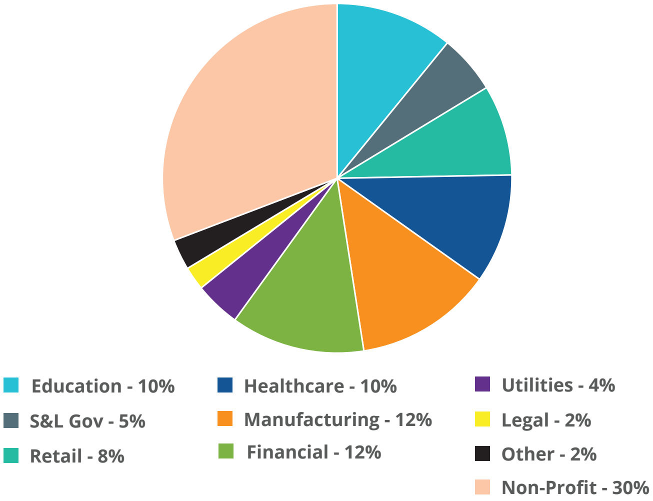


FIGURE 3:

[WHAT CHANGES TO WORKLOAD DELIVERY DO YOU ANTICIPATE OVER THE NEXT 3 YEARS?]

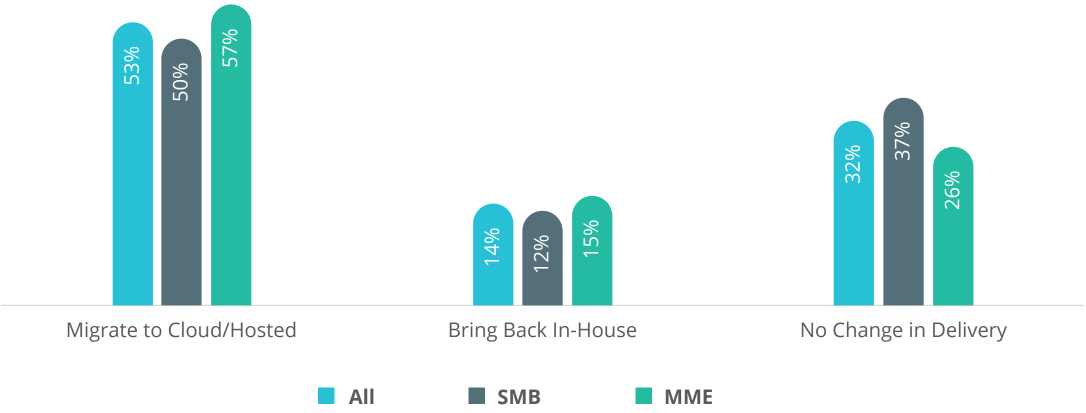


FIGURE 4:

[HOW MANY TOTAL HOURS DAILY (ACROSS ALL STAFF) ARE SPENT MANAGING YOUR BCDR SOLUTION(S)?]

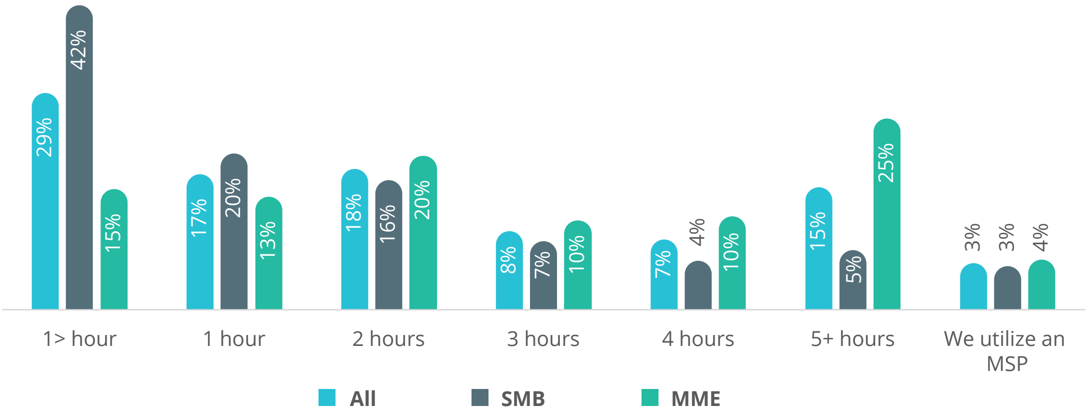


FIGURE 5:

[WHICH OF THE FOLLOWING HAVE YOU IMPLEMENTED TO PROTECT YOUR ENVIRONMENT CYBERTHREATS? SELECT ALL THAT APPLY]

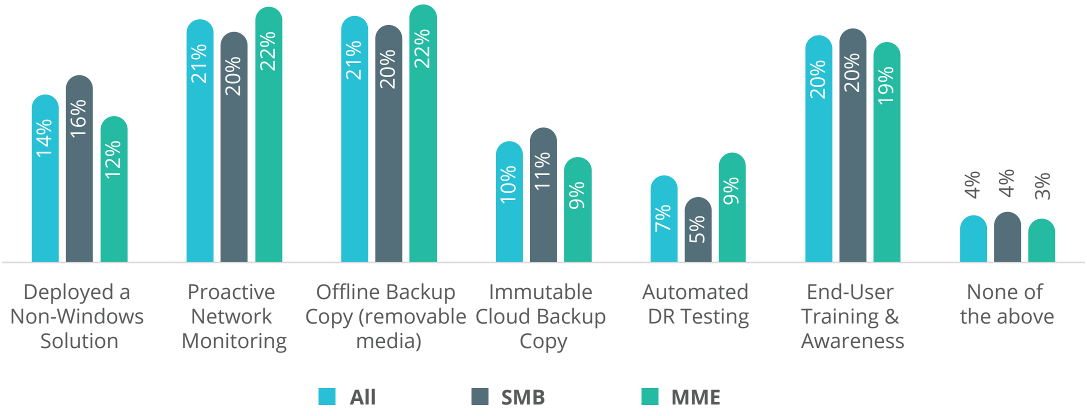
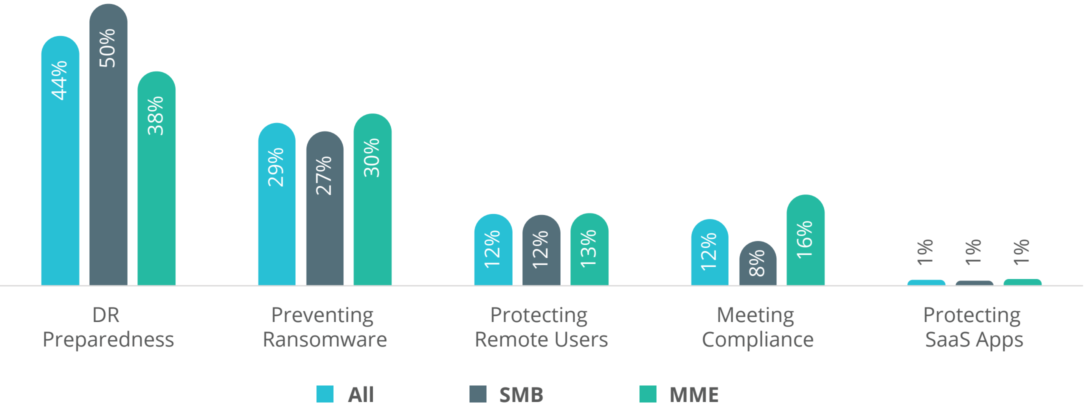


FIGURE 6
[OVER THE NEXT YEAR, DO YOU EXPECT YOUR IT BUDGET TO:]



IF YOU'RE INTERESTED IN LEARNING MORE

Contact your Unitrends expert

AlanFink

01635225262

alan.fink@prianto.com

SOURCE

[1] https://www.cloudwards.net/cloud-computing-statistics/

[2] https://www.imf.org/en/Publications/WEO

[3] https://www.apollotechnical.com/statistics-on-remote-workers/

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY