

datto

Datto's
**Global State of the
MSP Report:
Looking Ahead to 2023**



Introduction

Datto surveyed more than 1,800 managed service providers (MSPs) worldwide to find out what makes them tick, what keeps them up at night and where they think their biggest growth opportunities are. Of those surveyed, less than 20% were active Datto partners. The other 80+% were comprised of MSPs from all different shapes and sizes around the globe.

There were a number of results that stood out, especially when compared to previous Datto surveys. For the second year in a row, respondents said that competition is their top challenge. As to why, answers vary from challenges in marketing to market saturation. The MSP market sentiment continues to remain strong, and nearly all respondents still believe it is a good time to be an MSP.

Interestingly this year's survey saw an 11% increase in break-fix revenue, which some of our industry experts believed was more about a conceptual change to the break-fix model. Nearly all MSPs now offer some flavor of managed security services, and they too see an evolution toward solutions that help mitigate and monitor for attacks as well as recover from them.

Finally, most MSPs expect that at least 75% of client total workloads will be in the cloud over the next three years. This is up 25% from last year's report.

MSPs continue to be the core of the IT channel and Datto's business. They are essential service providers for millions of small and midsize businesses (SMBs) worldwide. We hope that this report sheds light on this industry that continues to thrive.



Key Findings



Cloud-based infrastructure design and management and office productivity software services are the top managed services currently offered.



There is a big opportunity for new solution offerings with a strong intent to add new solutions in the next year across the board, primarily around collaboration software (26%) and storage design and implementation (25%).



The hybrid workforce (remote + office) is here to stay. There are a few MSPs that have clients whose workforces are fully remote, but most have settled into a permanent hybrid plan. MSPs will now need to ensure all offerings accommodate this model.



Revenue associated with managed security services seems to be shifting to break-fix across regions. Reasons vary, but many feel this shift is not the same as the break-fix the industry dealt with 20 years ago. Break-fix has conceptually changed to more of a co-managed service offered by MSPs to help over-burdened IT departments in larger companies stay afloat.

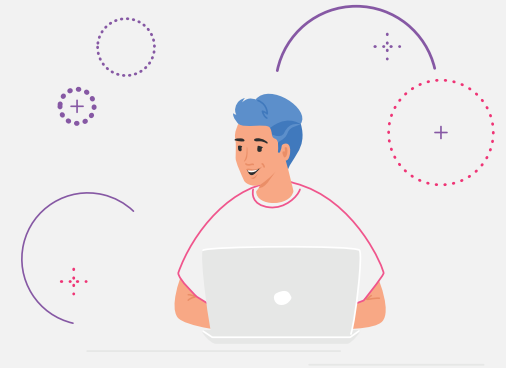


Cybersecurity is still a very large area for growth. While services for ransomware and phishing/email security remain the top focus for MSPs, others are finding further growth offering services around expanding reporting, auditing, training and policy building for clients.



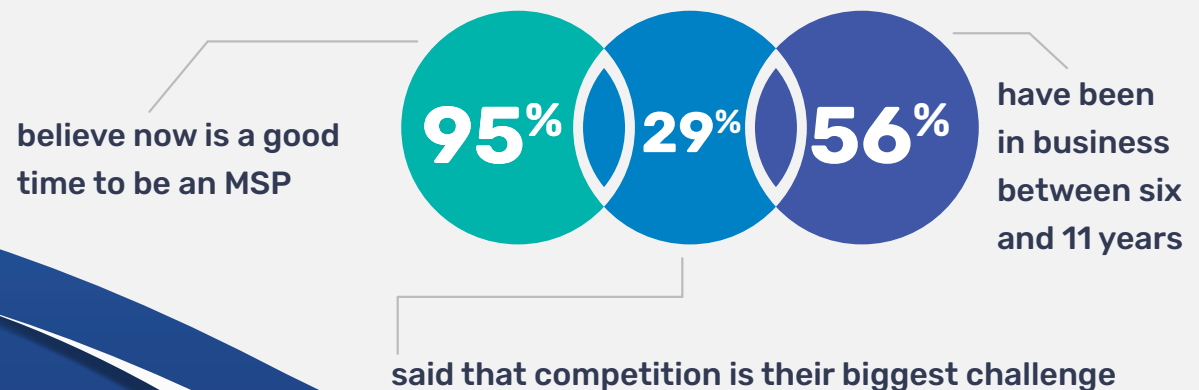
The Business of Managed Services

Just over half of respondents said they have been in business between six and 11 years. However, nearly a quarter reported that they've been in business for less than five years, indicating the industry is still attracting newcomers. This makes sense considering that 95% of respondents said now is a good time to be in their industry, and 82% expect revenue will increase over the next three years.

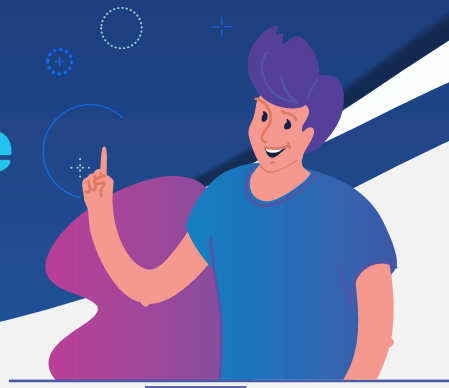


That being said, competition is getting stiffer. For the second year in a row, MSPs have said competition was their biggest challenge (29%). Conclusions as to why vary from challenges MSPs face with finding time to market their business to the rapid increase of MSPs in the market leading to stronger competition in finding and retaining clients. It will be interesting to see how this plays out over the next few years as the market continues to grow.

Even with competition being the biggest challenge, 95% of respondents said they believe now is a good time to be an MSP. Many MSPs also agree (80%) that their local or federal government is providing good support related to cybercrime. Sentiment is growing (64%) around the preference of using fewer vendors to meet technology needs.



Who MSPs Serve



The majority of MSPs reported serving businesses with 20 to 200 employees. More specifically, the 50 to 100 employee range was most common (20%), followed closely by 25 to 50 (17%) and then 100 to 150 (13%). Outside of the 20 to 200 employee range, there was a sharp drop-off on either end. Very few respondents serve clients with fewer than 10 employees (0) or more than 300 employees (3%).

On average, the clients of the responding MSPs spent \$13k per year on managed services – 25% fell within the \$5K to \$10K range, and another 28% spent \$10K to \$15K. Some clients spent an even larger amount with responding MSPs, though 20% spent between \$15K and \$20K, and another 12% spent between \$20K and \$30K.

71% of MSP clients have between 20 and 200 employees, down from 84% in 2021

The majority of MSP clients are still spending between \$5,000 and \$15,000 per year on managed services

On average, MSPs serve SMBs across three to five industries vs. five to six in 2021

High Tech (47%), and Healthcare (44%) were the top industries MSPs report serving. Telecom, which was top of the list in 2021, dropped from 46% to 41%, still landing in the top three. In general, MSPs across the globe continue to target a very wide variety of verticals. Many respondents have clients in Travel/Transportation, Manufacturing, Professional Services, Education, Energy, Media/Entertainment and Financial Services.

Geo trend:

While High Tech and Healthcare are the **top industries** across all geographies, MSPs in Europe are more likely to serve the **Travel/Transportation industry (41%)**, while in North America, they are **more likely to serve Construction (32%), Architecture/ Design (27%)** and **Government (14%)**.



Managed Services: Revenue by the Numbers

%



Annual Revenue

Nearly 36% of respondents reported annual revenues between \$1 million and \$5 million, and 32% said they had annual revenue of less than \$1M. However, 8% of respondents had annual revenue of over \$10 million and 5% over \$20 million.

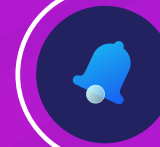
Break-fix has typically reflected MSPs having flexibility built into their contracts to charge extra for projects that fall outside of their normal responsibilities. Others use it for legacy clients that have not been converted over to managed services. This increase in break-fix could also be attributable to a shift to new business opportunities.

Geo trend:

Europe is slightly less likely to offer co-managed services; the top co-managed service in every region is BCDR, which is highest in North America.



Nearly 36% of responding MSPs had revenue **between \$1 million and \$5 million**



56% of respondents' total revenue came from recurring services



35% of revenues came from break-fix or project-based work

Annual Revenue

Even with the challenges, market sentiment is still quite positive. 82% of MSPs that responded to the survey said that they expect revenue growth to continue over the next three years and that they have set specific growth goals.



94%

of MSPs set specific goals for their business



82%

expect their revenue to increase over the next three years



74%

anticipate growth of more than 5%



Geo trend:

Three out of five MSPs experienced an increase in revenue in the past 12 months, although one in 10 in APAC said their revenue decreased. Overall, most MSPs expect their revenue to increase over the next three years, although those in APAC are most likely to think it will stay the same.

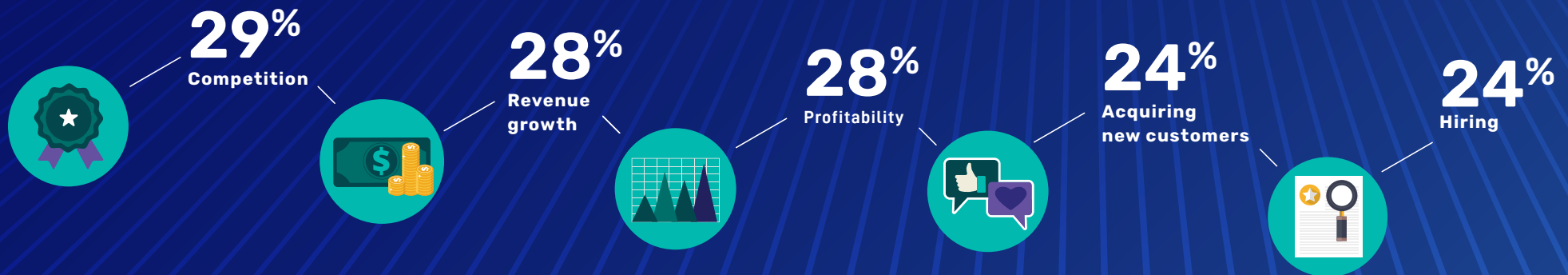
What's Keeping MSPs Up at Night?

The top challenge for respondents is once again competition, followed very closely by revenue growth, profitability and acquiring new customers.



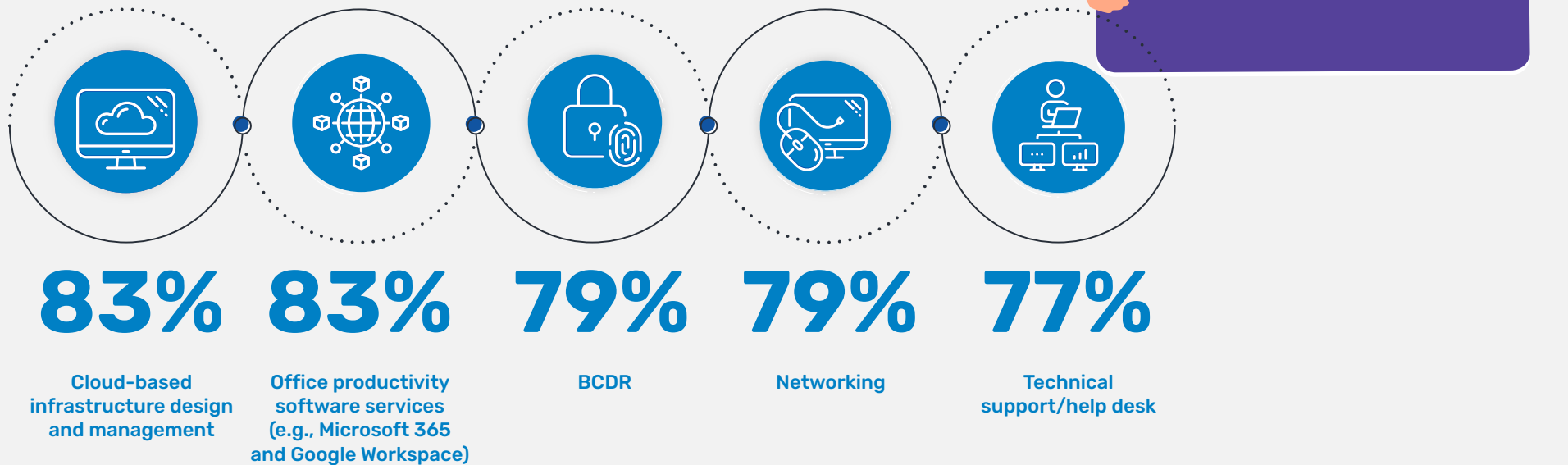
Competition remains the top challenge for MSPs year over year. This isn't particularly surprising as the MSP space continues to grow and the landscape becomes more competitive. It is interesting that MSPs remain quite bullish about revenue growth even though it also ranks highly as a challenge year over year. It could be argued that SMBs are becoming more acquainted with the value of an MSPs' services, creating stronger competition among MSPs as SMBs seek out the MSP with the best services and tools to fit their needs.

Additionally, as many MSPs speak consistently to the challenges associated with sales and marketing, specifically finding the optimal tools, time and strategy that provides high-quality leads could also be contributing to the challenge of remaining competitive and growing revenue.



Current Managed Services Offerings

90% of MSPs responding to the survey now offer cloud-based infrastructure design and management, indicating that the shift to the cloud continues to be strong among SMBs. Many predicted COVID-19 would accelerate migration to the cloud, and that continues to be the case. Traditional MSP offerings of Networking, Business Continuity and Disaster Recovery (BCDR) and Technical Support rounded out the top five services offered.



Anticipated growth areas for managed services offerings (within the next 12 months)

| | |
|-----|---|
| 26% | Collaboration software |
| 25% | Storage design and implementation |
| 24% | Incident response and forensics |
| 23% | Business intelligence or analytics software or services |
| 22% | Endpoint threat detection and response |



Managed Security Services – Solutions that Positively Impacted MSP Businesses



MANAGED SECURITY CURRENTLY OFFERED

While ransomware and email security issues remain top priorities for many MSPs, new players and tactics continue to proliferate. Many MSPs are looking toward tools that not only address issues after an attack but, more importantly, help monitor networks to mitigate their risk. A third of respondents in all markets still believe security solutions continue to present new business opportunities. The top Managed Security Service currently offered is email security. Several areas, including security framework and compliance auditing and advanced endpoint security, are expected to be offered over the next 12 months.

76%

Email security

71%

Password policy management

69%

Security framework and compliance auditing

| | |
|-----|--|
| 67% | Two-factor authentication (2FA) |
| 65% | Firewall (Basic) |
| 62% | Remote access technologies (e.g., VPN) |
| 62% | Advanced endpoint security (i.e., next-gen antivirus or endpoint detection and response) |
| 57% | Identity access management (IAM) and single sign-on (SSO) |

MANAGED SECURITY SERVICES PROJECTED TO BE ADDED OVER THE NEXT 12 MONTHS

30% Managed detection
& response

Privileged
access
management **29%**

30% Dark web
monitoring

Endpoint detection
and response (EDR) **28%**

29% Web content
filtering

Patch
management **28%**

29% Compliance
monitoring

Incident response
(IR) & forensics **28%**



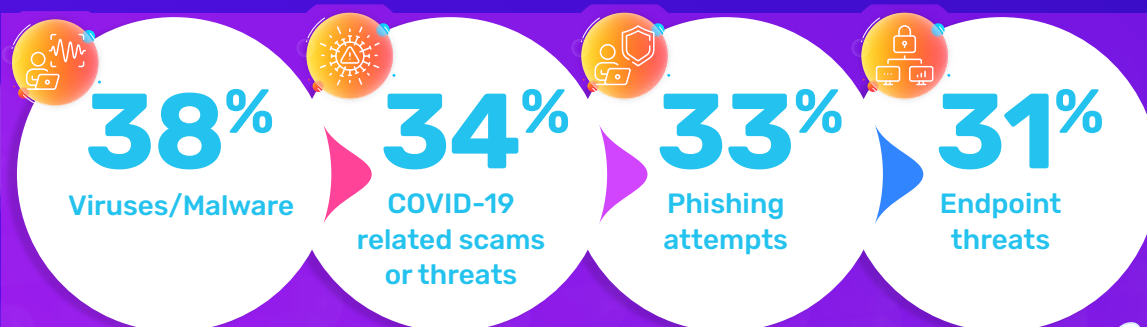
Top Cybersecurity Concerns and Issues



Computer viruses, followed by COVID-19 related scams, phishing messages, and endpoint threats are the top cybersecurity issues faced by MSPs. Yet only two in three say they have the antivirus protection tools in place currently; tools poised for highest growth are those addressing wiper malware, spyware, hackers, identity theft and phishing.

Although technologies are keeping pace with combating breaches, MSPs still struggle with security expertise in hiring skilled security specialists and grappling with the complexity of current security products.

Top Security Concerns



THE TOP BARRIERS TO OFFERING CYBERSECURITY SOLUTIONS ARE

| | |
|-----|--|
| 42% | Hiring skilled cybersecurity professionals |
| 41% | Complexity of cybersecurity products |
| 38% | Managing too many different cybersecurity products |
| 33% | Insufficient training of existing staff |

TOP TOOLS FOR GROWTH

| | |
|-----|--------------------------------|
| 67% | Antivirus |
| 55% | Endpoint threats detection |
| 54% | Anti-phishing solution |
| 52% | Password protection |
| 51% | Remote tool threat monitoring |
| 49% | Ransomware protection |
| 48% | COVID-19 scam threat detection |
| 47% | Identity management |



Managed Security Services Security and Compliance Standards



The use of security frameworks to help address compliance issues continues to grow. Each framework has pros and cons, and many MSPs tend to work with more than one framework, particularly when implementing security audits or building security policies for clients.

TOP COMPLIANCE FRAMEWORKS

| | |
|-----|-------------------------------------|
| 37% | CMMC |
| 27% | CIS |
| 24% | NIST CSF |
| 21% | ISO 27001/2 |
| 15% | SOC II |
| 19% | ASD Essentia I 8 |
| 18% | PCI-DSS |
| 17% | HIPAA |
| 16% | NCSC National Cyber Security Center |



Four in five MSPs currently provide Security Audits and Education Training for clients, with nearly as many creating internal security policies for them. Internal security policies are less used currently but are set to see the most growth in 2023.



Currently offered



Planning to add in 2023

| | |
|-----|--|
| 18% | Security audits for clients |
| 19% | Security education training for clients |
| 33% | Creation of internal security policies for clients |

SMB Workloads Continue Shifting to the Cloud

Cloud Integration



The cloud solution opportunity is similar to that of security solutions in that it continues to grow. However, some MSP clients are resistant to move to the cloud due to compliance, security or budgetary concerns.

Still, 95% of MSPs see new market opportunities in cloud integration with more clients looking to the cloud for better storage design and implementation as well as to provide better productivity and collaboration across teams.

About half of MSP respondents expect more than three-quarters of their workloads to be in the public cloud within three years, a 25% increase from last year's survey.

Growth is even higher in North America, as only 7% of MSP workloads are currently in the cloud, yet 75% of respondents expect this to rise to 25% within three years.

That said, North America has more reasons for keeping workloads on-prem such as resistance to converting spend, stricter compliance requirements, and more digital transformation than they are willing to undertake.

98%

of MSP clients are using the cloud in some capacity

76%

of MSP clients have shifted more than half of their workloads to the cloud, up significantly from last year's 50%

99%

of MSPs expect to have at least half of all client workloads in the cloud in the next three years, an increase from 93% in 2021

Workloads in the Cloud



Clients adopting Infrastructure as a Service (IaaS) have moved all types of workloads to the cloud. Email servers, databases and application servers were the most common (and expected to remain so in the next three years).

For clients that have migrated from on-prem to the public cloud, databases, web servers, and file servers continue to be the most commonly moved into the cloud.

As to where these workloads are and how much? Amazon AWS and Microsoft Azure hold the majority of client workloads.

77%
Email
Servers

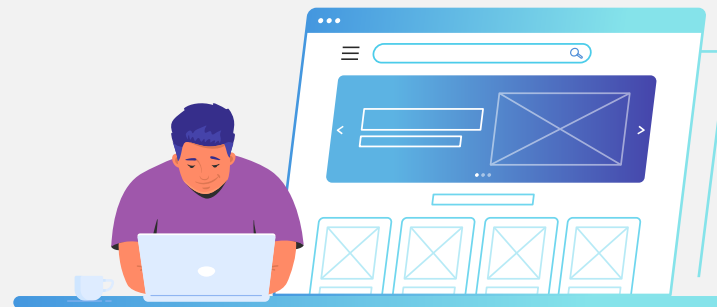
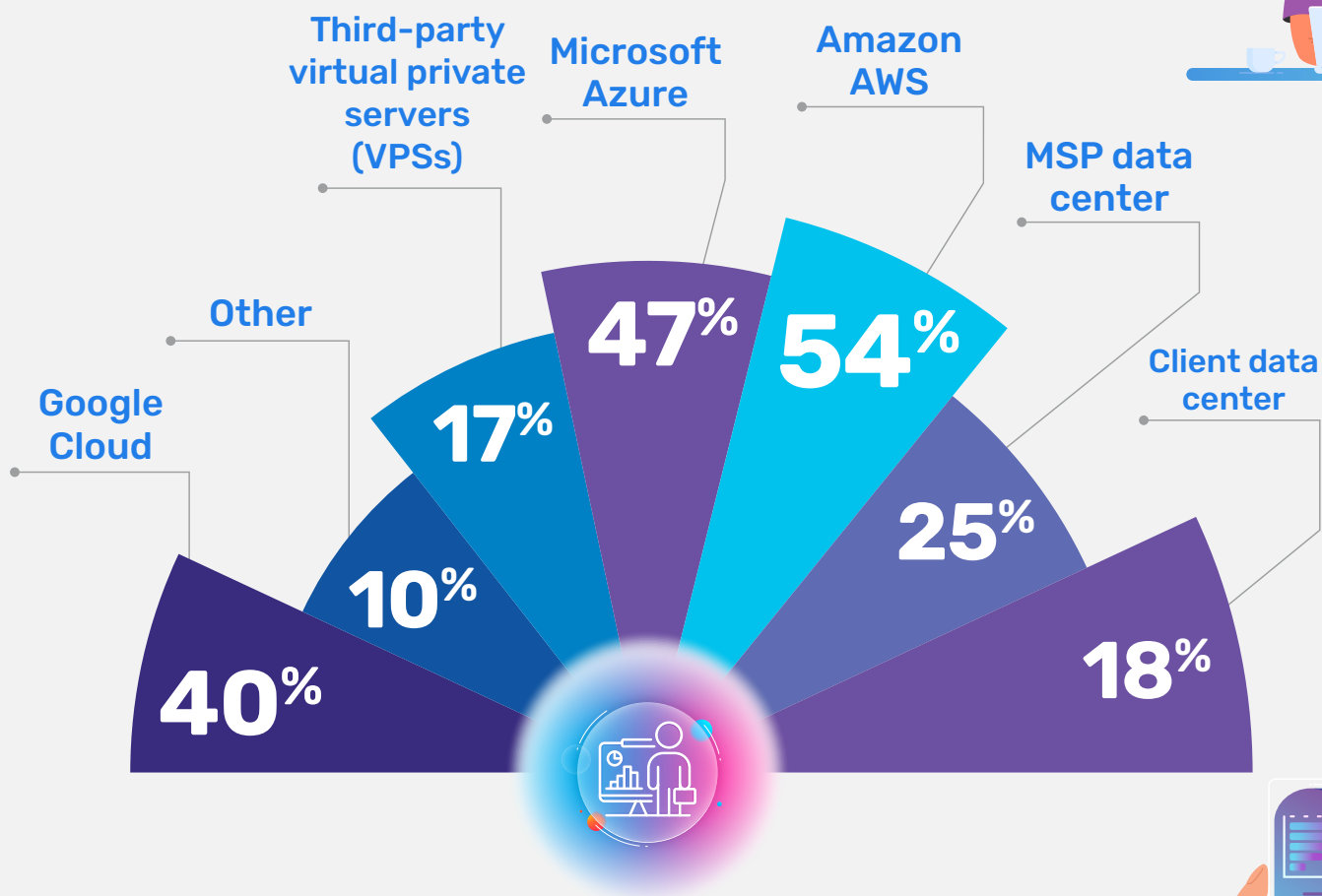
77%
Database
Servers

68%
Application
Servers

59%
DNS

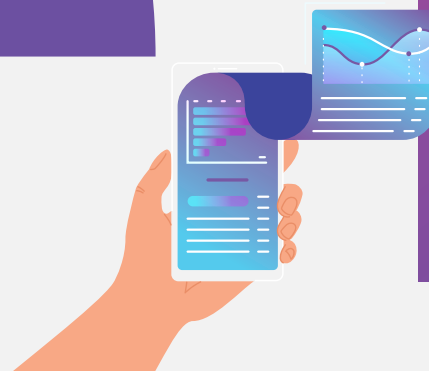
33%
LDAP/Active
Directory

WHERE MSPS EXPECT WORKLOADS TO BE



Geo trend:

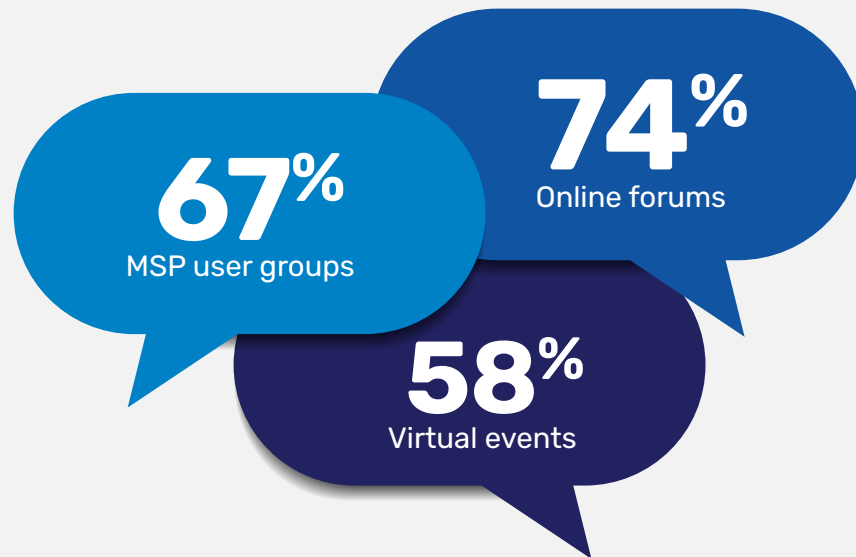
In APAC, six in ten of the responding MSPs expect 73% or more of databases to be in the cloud by 2024. By comparison, **only four in ten North American MSPs expect 79% of databases in the cloud.** APAC is ahead of the curve with application servers as well. Among respondents, they have the largest percentage of app servers in the cloud today, and more than half expect **75% or more to be in the cloud in two years.**



How MSPs Network

When in-person events were canceled worldwide in 2020 due to COVID-19, responding MSPs went online to connect. As the world continues to open and in-person events re-emerge in full force, it will be interesting to see how this effects online forums and virtual events.

It's worth noting that passive networking remains a popular approach. Perhaps respondents prefer interacting with peers and vendors on their own time via forums rather than sitting for a full, scheduled virtual event. This could also be attributed to the limited time MSPs have and to the comfort level MSPs have gained communicating virtually over the past two years.



Geo trend:

Online community forums are used more in APAC (77%) than in other markets for networking with peers and vendors.



Key Takeaways



Competition continues to be the top challenge facing MSPs. Reasons for this range from challenges around marketing to increased options of MSPs and the tools and services offered from which clients can choose.



Security needs are still very strong and growing fast. Ransomware and phishing/email security remain the top focus for MSPs, and many are finding further growth offering services around reporting, auditing, training and policy building for clients.



Break-fix is back. It has re-emerged as co-managed services, which enables MSPs to get a foot in the door with larger business by focusing on a specific IT challenge.



Most MSPs expect at least 75% of client workloads will be in the cloud by 2023.



Research Approach

This report is based on a survey of over 1,800 MSPs worldwide. It was conducted by Strategy Analytics, an independent research firm based in Boston, Massachusetts.

Methodology:

- 15-minute online survey
- Ending sample is a total of n= 1,897 globally

Survey respondents

83% Not Datto partners

17% Datto partners

Respondents:

- Must be from a managed service provider (MSP)
- Must be a decision-maker or influencer for solutions for their company

Regions:

n=625 North America

n= 414 U.S.

n= 211 Canada

Regions:

n=736 Europe

n= 160 U.K./Ireland

n= 156 Benelux
(Belgium, Netherlands, Luxembourg)

n= 159 DACH
(Germany, Austria, Switzerland)

n= 104 ROE
(France, Italy)

n= 157 Nordics
(Denmark, Norway, Sweden)

Regions:

n=536 APAC

n= 106 Australia

n= 109 New Zealand

n= 104 Singapore

n= 107 Indonesia

n= 110 Philippines

Glossary of Terms

Business email compromise (BEC): Sometimes called email account compromise (EAC) BEC is a scam that utilizes legitimate (or freshly stolen) email accounts from a trusted business to fraudulently acquire money, personal information, financial details, payments, credit card numbers and other data from a business. These scams also target businesses that use wire transfers, foreign suppliers and other invoice transactions.

Break-fix IT: IT services delivered on a project basis. Many MSPs started as break-fix IT providers, and some portion of their revenue may come from one-off projects billed on an hourly basis. This model has conceptually changed this past year as MSPs look to target IT for larger business', an area we dig into in this report.

Co-managed IT: A model in which multiple parties are responsible for a single organization's IT needs. This might mean an MSP and an MSSP working together, as outlined in the example above. Or, it could mean an MSP partnering with an organization's internal IT team.

Cyber resilience: Cyber resilience is a measure of strength in preparing for, operating through and recovering from a cyberattack. It relies on the successful ability to identify, protect, detect, respond and recover quickly from any cyber event, and it combines cybersecurity, business continuity and incident response.

Dark web: Part of the internet that can be accessed only with special software. It is intentionally hidden from search engines, and uses masked IP addresses allowing users and website owners to remain secret. It is used mostly for criminal activities.

Endpoint security: The connection of endpoint devices such as laptops, tablets, mobile phones, internet-of-things devices and other wireless devices to corporate networks creates attack paths for security threats.

MSP: Managed service provider. A third-party IT contractor or firm that delivers an agreed-upon set of services for a monthly or annual fee.

MSSP: Managed security service provider. Due to the complexity of IT security, MSSPs focus on it exclusively. Many MSPs partner with MSSPs for their security expertise.

SMB: Small and midsize businesses. According to Gartner, "small businesses are usually defined as organizations with fewer than 100 employees; midsize enterprises are those organizations with 100 to 999 employees."

Supply chain attack: A cyber-attack that seeks to damage an organization by targeting less secure elements in the supply chain.

About the Report

Datto's Global State of the MSP Report,: Looking Ahead to 2023 is based on statistics pulled from a survey of roughly 1,800 MSPs worldwide. The survey was conducted by Strategy Analytics on behalf of Datto.

Credits

This report was created by (a-z): Ona Blanchette, Elizabeth Fichtner, Sindi Karlowicz, Amy Newman, Holly Pateman, and Eileen Weinberg of Datto, Inc. Research was conducted by Strategy Analytics. Illustrations were created by MRPJ Designs, Inc.

Re-use

We encourage the re-use of data and text published in this report under the terms of this Creative Commons Attribution 4.0 International License. You are free to share and make commercial use of this work as long as you attribute the Datto State of the MSP Report Looking Ahead to 2023 as stipulated in the terms of the license.

About Datto

As a leading global provider of security and cloud-based software solutions purpose-built for Managed Service Providers (MSPs), Datto, a Kaseya Company, believes there is no limit to what small and medium businesses (SMBs) can achieve with the right technology. Datto's proven Unified Continuity, Networking, Endpoint Management, and Business Management solutions drive cyber resilience, efficiency, and growth for MSPs. Delivered via an integrated platform, Datto's solutions help its global ecosystem of MSP partners serve over one million businesses around the world. From proactive dynamic detection and prevention to fast, flexible recovery from cyber incidents, Datto's solutions defend against costly downtime and data loss in servers, virtual machines, cloud applications, or anywhere data resides. Since its founding in 2007, Datto has won numerous awards for its product excellence, superior technical support, rapid growth, and for fostering an outstanding workplace. With headquarters in Miami, Florida, Datto has global offices in Norwalk, Connecticut, as well as Australia, Canada, Denmark, Germany, the Netherlands, and the United Kingdom.

Learn more at www.datto.com.

datto