2020
MSP BENCHMARK
SURVEY RESULTS REPORT

Kaseya®

INTRODUCTION

The managed services market was valued at around $186 billion (U.S. dollars) in 2019, with forecasts suggesting that this number could grow as high as $356.24 billion by 2025.[1] Note that these numbers reflect the state of the market prior to the COVID-19 pandemic. While it is too early to gauge the full economic impact, we anticipate competition to increase and these numbers to change. One thing is certain. The managed service provider (MSP) market is expanding rapidly as small and midsize businesses increasingly look to MSPs to manage their IT services and keep their data secure.

However, while some MSPs seem to get the hang of growing their business, others struggle since they spend a great deal of time looking for, training and retaining skilled technicians, dealing with inefficient remote monitoring and management (RMM) tools, failing to deliver the services promised and falling prey to cyberattacks.

Since most MSP professionals come from a technical background, they spend most of their time on IT, with their sales and marketing operations taking a backseat.

With much riding on their shoulders, MSPs need to be cautious of the tools they invest in, the services they provide and the service-level agreements (SLAs) they commit to.

The 2020 MSP Benchmark Survey Report takes a deep dive into the various aspects of how MSPs function, the challenges they face, the services they offer and their requirements.

MEET OUR RESPONDENTS

This report is based on the detailed data provided by more than 1,300 owners and technicians of MSP firms of all sizes, spread over 50 countries, with 76 percent of them from the Americas region (which includes the United States, Canada, Mexico and Puerto Rico).

While MSPs are generally advised to specialize in the service offerings they provide or in the markets they target to gain a competitive advantage, about two-thirds of respondents described their MSP profile as "general purpose" while 17 percent described their MSP profile as "managed security and service provider (MSSP)." "Network and data center focused" and "specialized by market vertical" were each selected by 10 percent of respondents.

76% Americas

16% EMEA

9% APAC

MSP Profile

59%
General Purpose

17%
Managed security service provider (MSSP)

10%
Network and data-center focused

10%
Specialized by market vertical

4%
Other
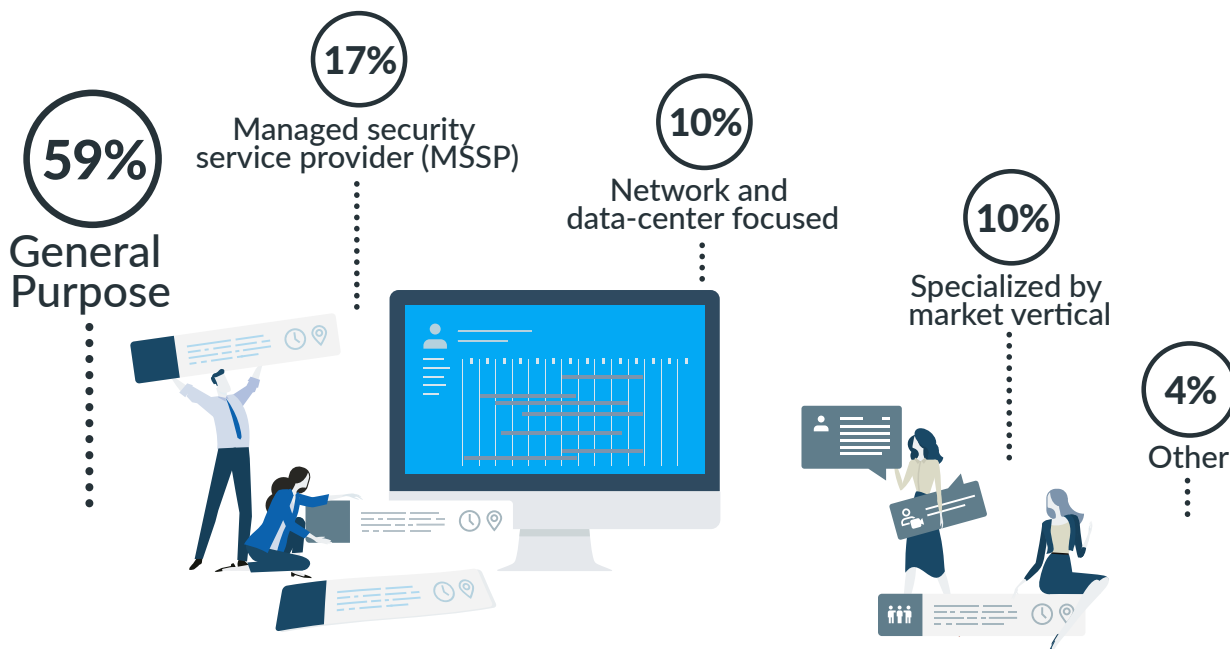
Company Size and Endpoints Managed

About 40 percent of respondents come from MSPs with fewer than 10 employees, and only 15 percent of respondents are from MSPs with more than 100 employees.

Company Size	Percentage
More than 100 employees	15%
51 - 100	8%
26 - 50	13%
10 - 25	24%
Less than 10 employees	40%
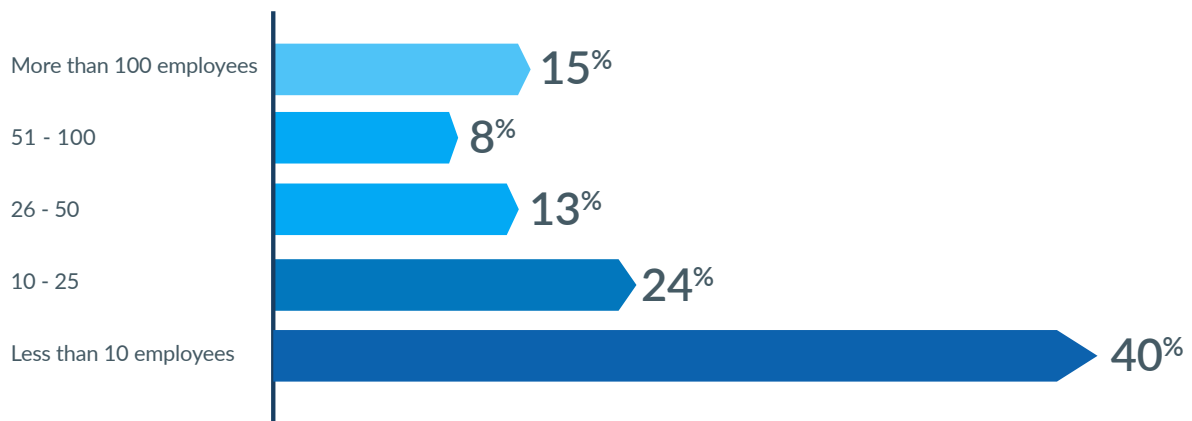
Employee Size vs. No. of Endpoints Managed

No. of employees	1 - 100 endpoints	101 - 500 endpoints	501 - 1,000 endpoints	1,001 - 3,000 endpoints	3,001 - 5,000 endpoints	5,001 - 10,000 endpoints	10,001 - 15,000 endpoints	More than 15,000 endpoints
Less than 10 employees	25%	37%	21%	14%	2%	0%	1%	0%
10 – 25	6%	12%	26%	39%	11%	3%	1%	2%
26 – 50	4%	6%	13%	34%	26%	12%	2%	3%
51 – 100	13%	9%	10%	25%	16%	16%	2%	11%
More than 100 employees	5%	13%	10%	19%	11%	14%	8%	21%

KEY FINDINGS

Six key themes emerged in the 2020 MSP Benchmark Survey results. Let's take a look at these MSP business challenges, concerns, risks and opportunities.

Top MSP Client Needs and Concerns

MSP customers, especially small businesses, have been facing increased security threats year over year. In the 2020 survey, **29 percent** of respondents listed "meeting security risks" as the top IT need for their clients. Another **14 percent** of respondents listed cybersecurity services as a top need.

Security and Backup Services Raise Revenue

With ransomware and malware attacks making headlines every day, MSPs are seizing the opportunity to protect their customers with security and backup services. Nearly three-quarters of respondents **(73 percent)** experienced a revenue increase in the past year through providing security services followed by backup and disaster recovery **(59 percent).**

The Need for Compliance Growing Stronger

Two-thirds of respondents report that their clients struggle to meet compliance requirements, while the need to provide compliance services has increased in the past two years for nearly **one-third** of the MSPs. Compliance is an area of business opportunity for MSPs.

MSPs Show Growth by Adding New Service Offerings to Portfolios

Nearly **90 percent** of respondents consider the expansion of their service offerings important. High-growth MSPs (with an average monthly recurring revenue (MRR) growth greater than 20 percent) have added about **4 to 5** new services to their offerings in the past two years.

Cloud Support Drops but Still Remains an Opportunity for MSP Growth

Public and private cloud adoption are among the top IT needs this year. However, MSP management of cloud environments has dropped from 70 percent of respondents in 2019 to **56 percent** for public cloud, and from 59 percent in 2019 to **49 percent** this year for private cloud.

There is room for growth in cloud management services — MSPs that manage their clients' public cloud environments, like Azure, AWS or Google, had **higher MRR growth**.

Integration Between Core IT Management Applications Matters to MSPs

MSPs have increasingly become aware of the importance of integration between their core applications, such as remote monitoring and management (RMM), professional service automation (PSA) and IT documentation. Nearly **70 percent** of respondents said that integration between their core IT applications is very important. In addition, **81 percent** responded that this integration could help their organization drive better bottom-line profits.

DETAILED FINDINGS

Mounting Security Needs of MSP Clients in 2020

29 percent of our respondents anticipate "meeting security risks" to be the top need for their clients in 2020. Not surprisingly, cybersecurity services, including antivirus, antimalware and ransomware protection, take the second spot in the list of top needs, bringing with it a growing demand to address these needs.

Top 6 IT Needs of MSP Clients

▶▶ **Meeting security risks**   **29%**

▶▶ **Cybersecurity services**
(e.g., AV, AM or ransomware protection)   **14%**

▶▶ **Public cloud adoption/migration/support**
(IaaS, PaaS, SaaS)   **9%**

▶▶ **Private cloud adoption/migration**   **6%**

▶▶ **Increasing the value of IT as a competitive**
advantage   **4%**

▶▶ **Increasing the level of IT automation**   **4%**

| MSP Client Needs for 2020	Americas	APAC	EMEA	All Respondents
➡ Meeting security risks	31%	21%	24%	29%
➡ Cybersecurity services (e.g., AV, AM or ransomware protection)	15%	8%	9%	14%
➡ Public cloud adoption/migration/support (IaaS, PaaS, SaaS)	7%	18%	11%	9%
➡ Hybrid cloud adoption/migration	7%	8%	10%	7%
➡ Private cloud adoption/migration	5%	15%	7%	6%
➡ Increasing the value of IT as a competitive advantage	4%	3%	4%	4%
➡ Increasing the level of IT automation	4%	7%	2%	4%
➡ Legacy system replacement (i.e., digital transformation)	4%	3%	5%	4%
➡ Supporting collaboration platforms (Office 365/Google Apps)	3%	3%	3%	3%
➡ Making the cost/budget of IT operations more predictable/manageable	2%	0%	1%	2%
➡ Audit and compliance reporting	2%	2%	1%	2%
➡ Data protection (cloud or onsite backup and recovery)	2%	2%	2%	2%
➡ Supporting mobile devices	2%	2%	3%	2%
➡ Outsourcing core IT functions (i.e., NOC service)	2%	3%	3%	2%
➡ Delivering higher service levels/IT service availability	1%	2%	2%	2%

Realizing the Ongoing Security Opportunity

Businesses have always been under attack, but the COVID-19 pandemic has unleashed a new wave of cybercrime with hackers routinely developing malware variants and exploiting software vulnerabilities, intensifying the need for a strong security posture.

For 77 percent of the participants, 10 to 20 percent of their clients have experienced at least one cyberattack within the 12 months prior to the survey. Hence, this reflects the state of affairs before the COVID-19 pandemic took hold.

Percentage of Clients That Have Experienced At least One Cyberattack Within the Past 12 Months

More than 80% **2%**

40% to 80% **6%**

20% to 40% **14%**

10% to 20% **77%**
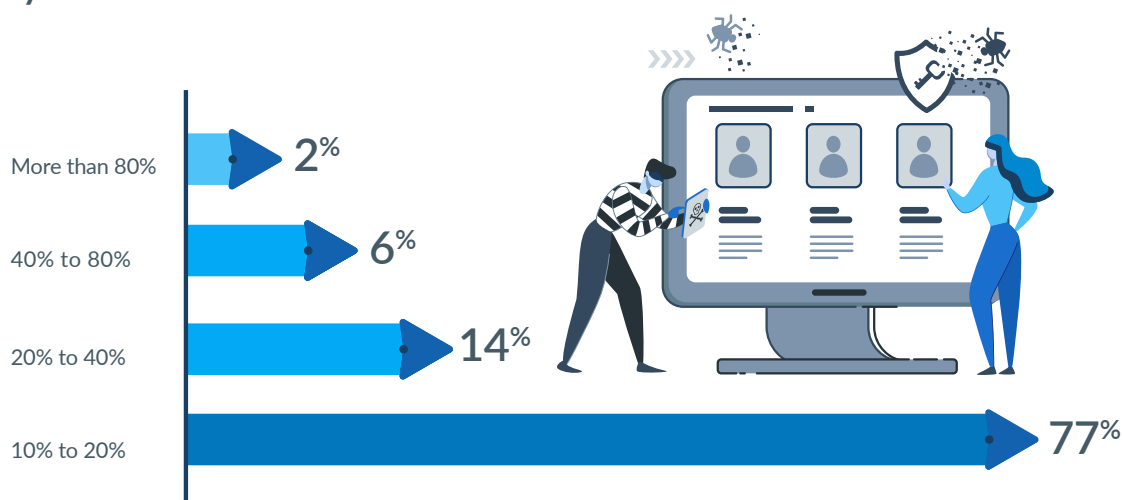
*When asked about downtime, about 60 percent of the participants said that their clients experienced data loss or downtime from an outage in the past year.*

Percentage of MSP Clients That Have Experienced Downtime From an Outage in the Past Year

YES! **60%**

NO! **40%**
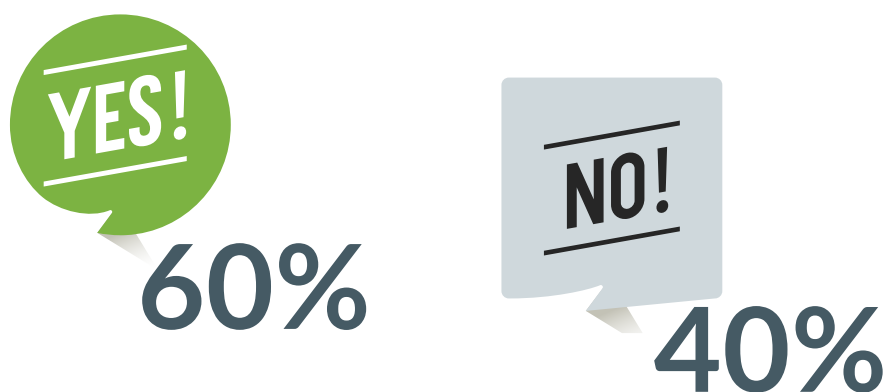
This has led businesses to opt for multiple security solutions, with 44 percent of respondents' clients using more than three.

## No. of Security Solutions MSP Clients Use

More than 7	**4%**
6 to 7	**6%**
4 to 5	**34%**
1 to 3	**56%**
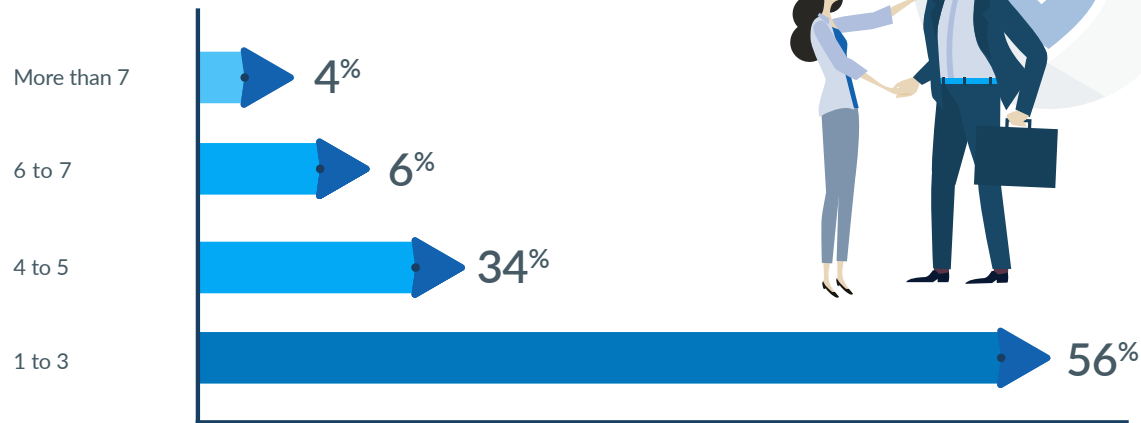
With businesses concerned about cybersecurity, they increasingly seek support from MSPs.

Almost all respondents (about 95 percent) have had either some or most of their clients turn to them for counsel on cybersecurity plans and best practices.

Clients Turning to MSPs for Counsel on Cybersecurity Plans

|	
All of our clients	**15%**
Most of our clients	**40%**
Some of our clients	**40%**
None of our clients	**5%**
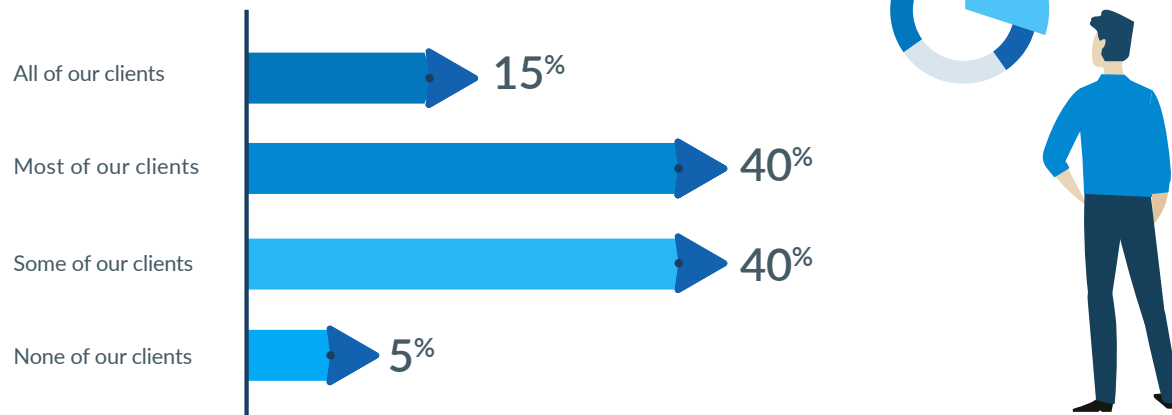
MSPs have seized this opportunity to provide much-in-demand security services, with almost three-quarters of participants reporting that the status of revenue has gone "up" for this category in the past 12 months.

Status of services revenue	Up	Down	Flat	Not applicable
Security	73%	2%	19%	7%
Backup and disaster recovery	59%	3%	30%	8%
Infrastructure Monitoring and Management	59%	3%	32%	7%
Desktop Support	57%	4%	31%	8%
Network and connectivity support	54%	3%	37%	6%
Hardware/Software Resale	51%	8%	31%	10%
Cloud management	47%	3%	28%	22%
Application management	29%	5%	41%	25%
Mobile device management	28%	6%	36%	30%

Security Services Provided

Antivirus and antimalware top the list of security services provided by MSPs, followed by firewall and VPN management.
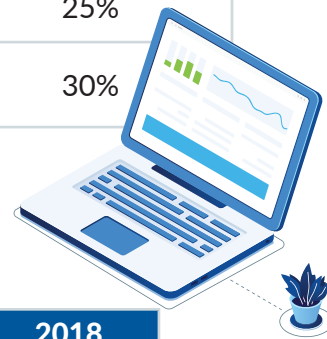
| Security services offered	2019	2018
Antivirus and antimalware	83%	80%
Firewall and VPN management	80%	81%
OS patching (Windows and Mac)	78%	80%
Managed firewall	76%	78%
Account creation/deletions	68%	59%
Password resets/self-service/password management	66%	62%
Active Directory repository (LDAP)	61%	58%
Two- or multi-factor authentication	57%	54%
Third-party application updating	54%	57%
Software management	53%	61%
Vulnerability and risk management	53%	53%
Real-time intrusion/threat detection	48%	49%
Network usage scanning (for unusual behavior)	43%	49%
Automated incident response	40%	33%
Single sign-on	39%	40%
Dark Web activity	31%	18%
High availability security operations center	24%	29%
We do not provide any of these services	3%	2%

It's Time for MSPs to Embrace the Cloud

Despite being a popular need, cloud support has gone down among MSPs. Only 56 percent of the participants responded "Yes" (as compared to last year's 70 percent) when asked if they were managing public cloud environments (e.g., Azure, AWS or Google) for any of their clients.

Percentage of MSPs Managing Public Cloud Environment for Clients

YES
56%
70%

NO
44%
30%

★ 2018 ★ 2019
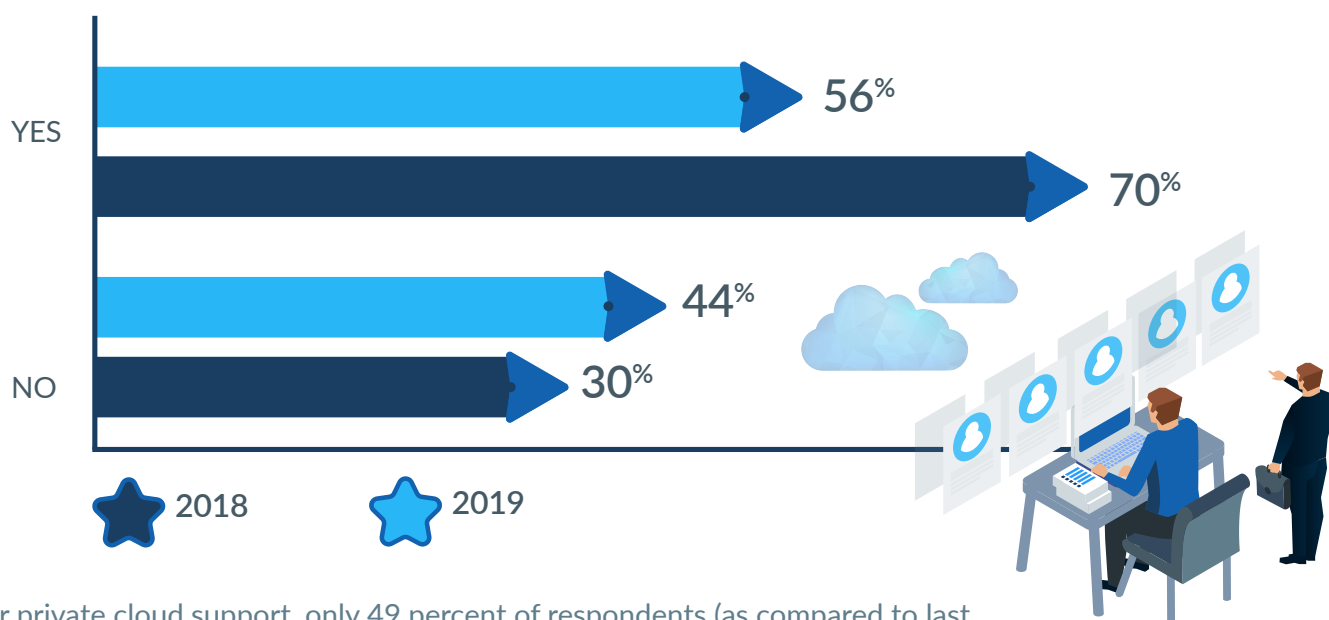
As for private cloud support, only 49 percent of respondents (as compared to last year's 59 percent) said that they are currently hosting client infrastructure on a private cloud.

YES
49%
59%

NO
51%
41%

★ 2018 ★ 2019
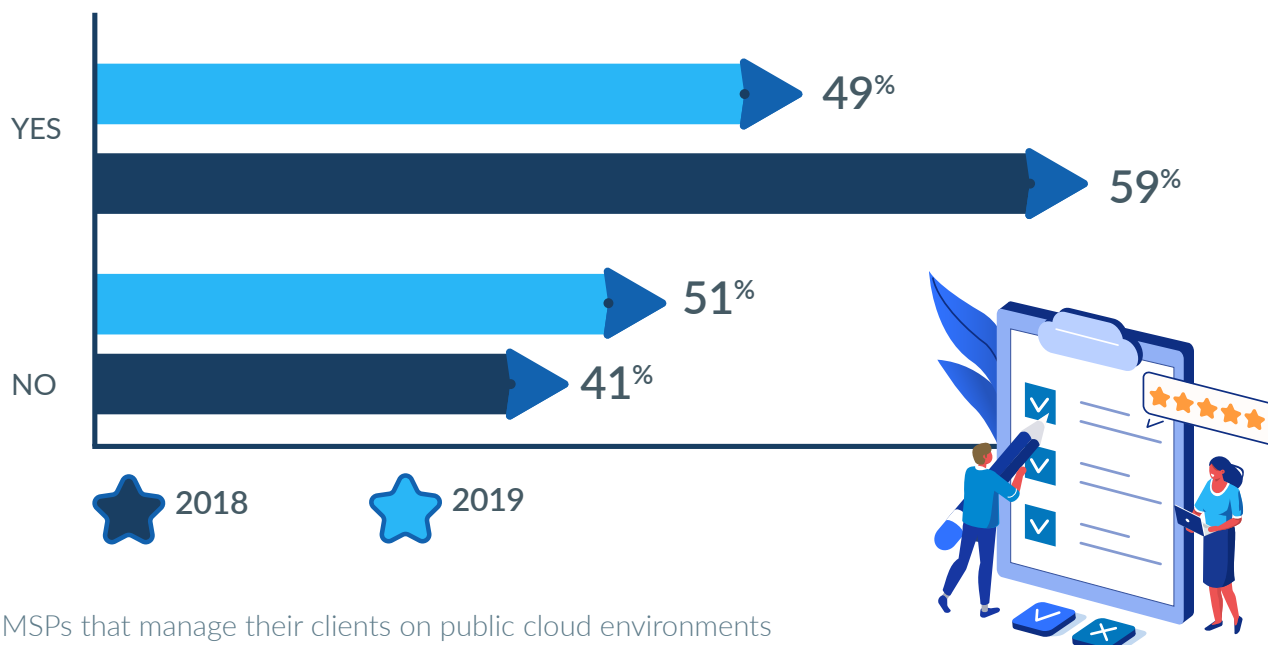
Also, MSPs that manage their clients on public cloud environments like Azure, AWS or Google, experienced slightly higher growth in MRR.

ARE YOU MANAGING ANY OF YOUR CLIENTS IN A PUBLIC CLOUD ENVIRONMENT?		
Average growth in MRR	**Yes**	**No**
Less than 0%	3%	8%
0% - 5%	20%	25%
6% - 10%	25%	26%
11% - 15%	21%	15%
16% - 20%	10%	8%
Greater than 20%	21%	18%

RMM Remains the Core Application for MSPs

Remote monitoring and management (RMM) software provides MSPs with much-needed visibility and control of their clients' IT environments. Without an RMM solution, managing their clients' IT would not be feasible. RMM, along with professional services automation (PSA) software, provides an end-to-end solution for managing IT operations.

For more than half of respondents (61 percent), RMM remains the most important application, followed by PSA (21 percent) and IT documentation (11 percent).

## Applications Core to MSP Operations

▶▶ **Remote Monitoring and Management (RMM)** **61%**

▶▶ **Professional Services Automation (PSA)** **21%**

▶▶ **IT Documentation** **11%**

▶▶ **Project Management** **3%**

▶▶ **CRM** **3%**

▶▶ **General Ledger/Accounting** **1%**

Application most important to MSP operations	APAC	EMEA	Americas	All respondents
Remote Monitoring and Management (RMM)	53%	60%	62%	61%
Professional Services Automation (PSA)	32%	14%	21%	21%
IT documentation	11%	9%	12%	11%
Project Management	2%	8%	2%	3%
CRM	2%	5%	2%	3%
General ledger/accounting	0%	4%	1%	1%

As discussed in the key findings, one-quarter of respondents say integration between their core MSP applications is "critical," while half describe it as "very important."

Importance of Integration Between Core MSP-Specific Apps

CRITICAL 23% 22%
VERY IMPORTANT 48% 47%
SOMEWHAT IMPORTANT 24% 26%
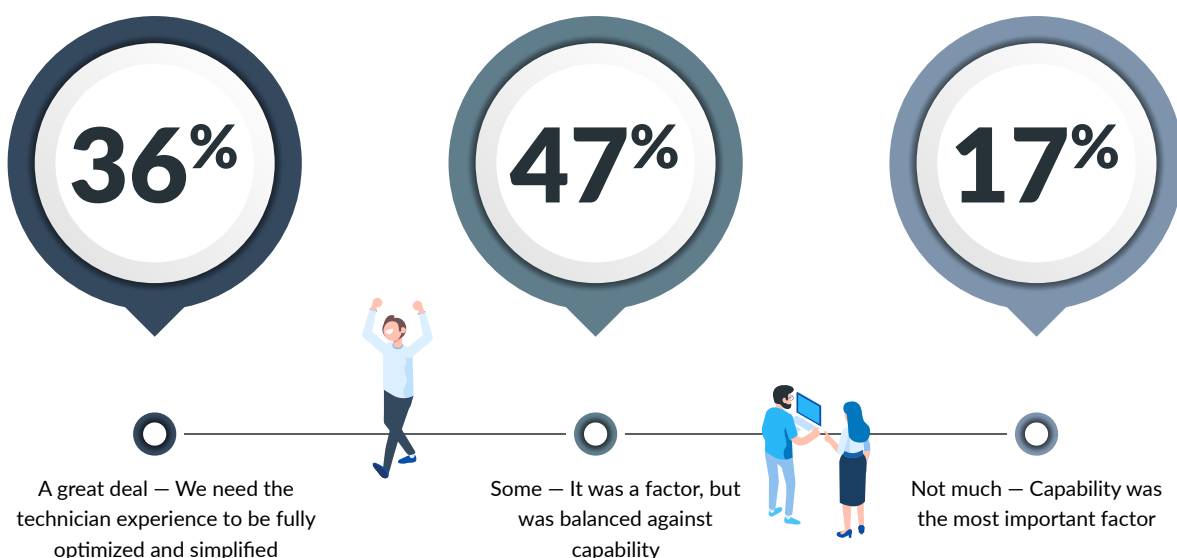NOT IMPORTANT 5% 4%
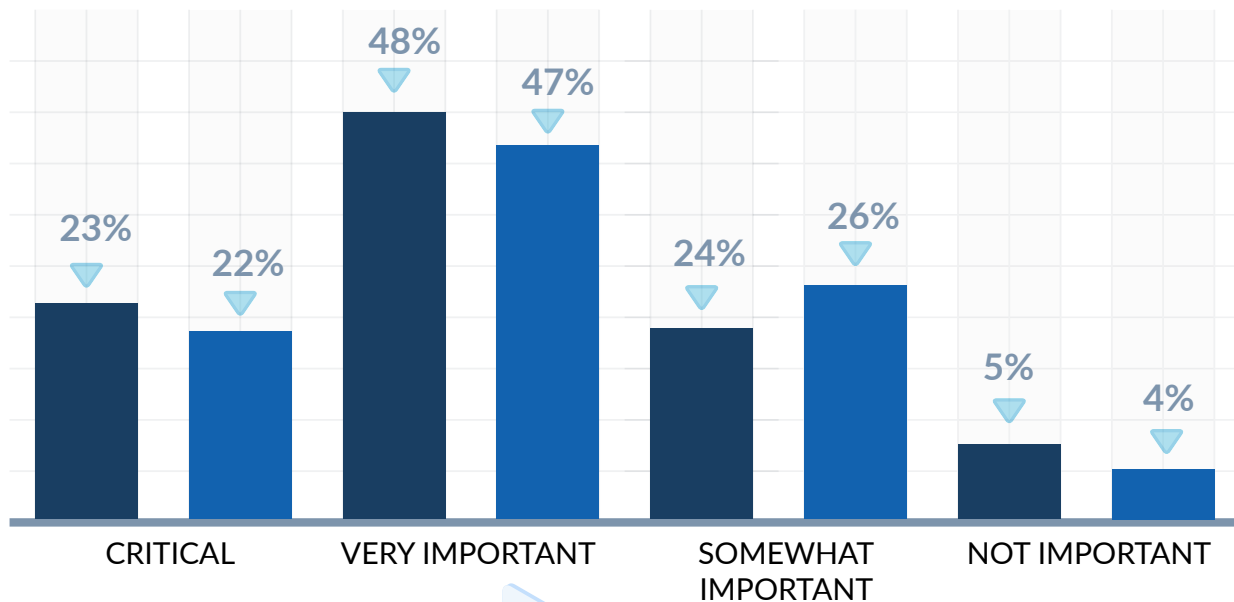
● 2019
● 2018

User Experience — A Game Changer?

Also, when asked if user experience impacted their RMM or PSA purchase decision, about 36 percent of respondents said that it had a great deal of impact, while 47 percent said that it had some impact but was balanced against capability.

The Extent of User Experience Factoring into RMM or PSA Purchase Decision

36%

47%

17%

A great deal — We need the technician experience to be fully optimized and simplified

Some — It was a factor, but was balanced against capability

Not much — Capability was the most important factor

SECURITY AND COMPLIANCE

Growing Security Risks Seen by MSPs

MSPs are very attractive targets for cyberattacks. Through their RMM solutions, MSPs have access to the IT environments of many clients. By breaching one MSP, cybercriminals can gain access to their clients' environments for ransomware and other types of attacks.

In our 2020 survey, 37 percent of participants said they felt their MSP business was more prone to cybercrime risk as compared to in 2019.
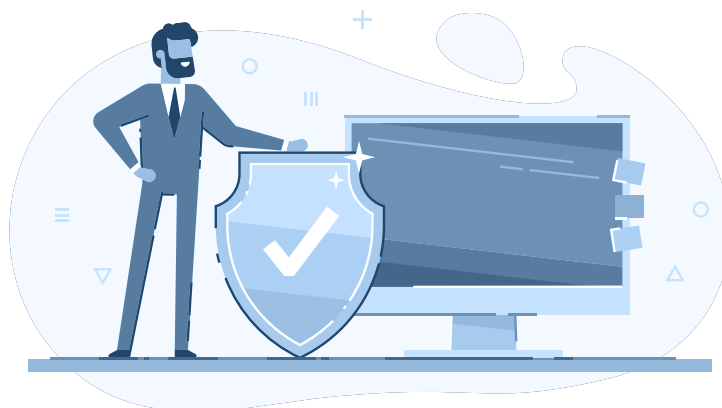
Cybercriminal Risk Level to MSPs

26% — More secure

27% — About the same

24% — More at risk

10% — Significantly more secure

13% — Significantly more at risk

| Significantly more secure | More secure | About the same | More at risk | Significantly more at risk |
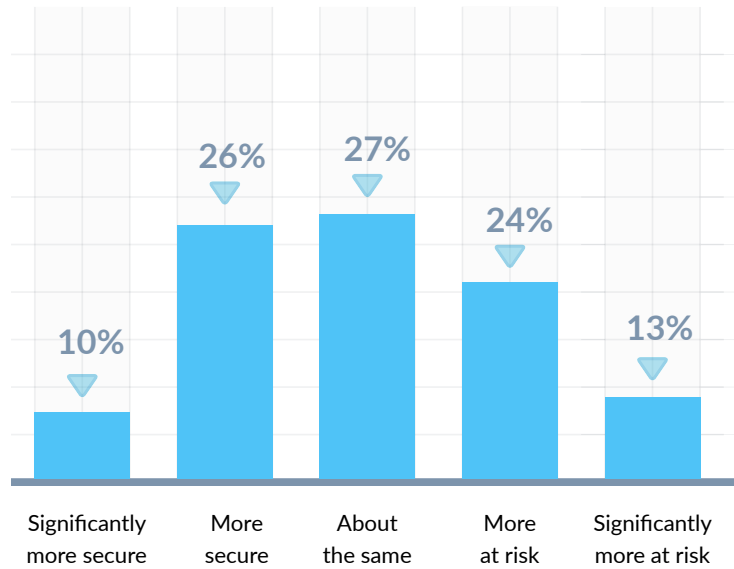
While there is no single solution to prevent data breaches, MSPs can strengthen their cybersecurity strategies to deter attackers. About 91 percent of respondents consider two-factor authentication (2FA) important for both their internal and customer systems.

2FA Important for MSPs and Clients

YES!

91%

NO!

9%
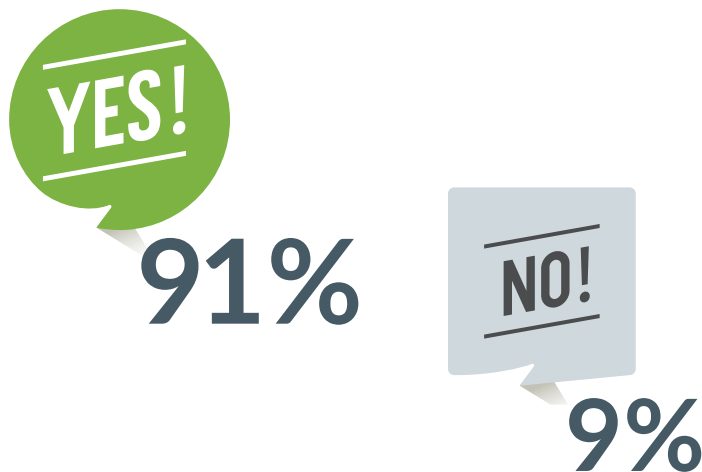
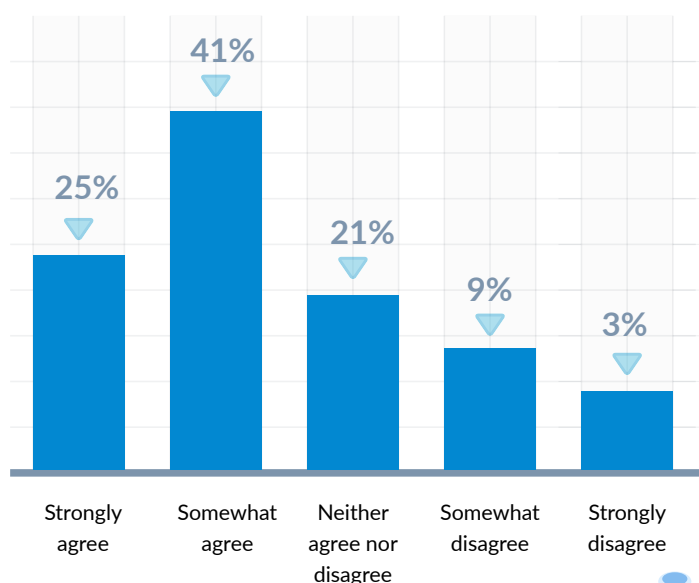## Finding Opportunity in Customer Compliance Challenges

One of the opportunities that MSPs should look at is compliance. With the increasing number of regulations, including the California Consumer Privacy Act (CCPA) and the New York Stop Hacks and Improve Electronic Data (SHIELD) Security Act, data privacy has become a necessity for small and large organizations alike. MSPs can leverage this opportunity to satisfy the need for maintaining compliance with these regulations for their customers.

66 percent of respondents say that their clients struggle to meet compliance requirements.

Statement: Our Customers Struggle to Meet Compliance Requirements for Their IT Operations

Nearly 60 percent of the participants say that their clients have sought their support for compliance services.

Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
25%	41%	21%	9%	3%

Extent to Which Clients Seek Out MSP Support for Compliance Services

More clients are requesting compliance services	A moderate number of clients are requesting compliance services	Fewer clients are requesting compliance services	We do not offer compliance services
32%	28%	23%	17%
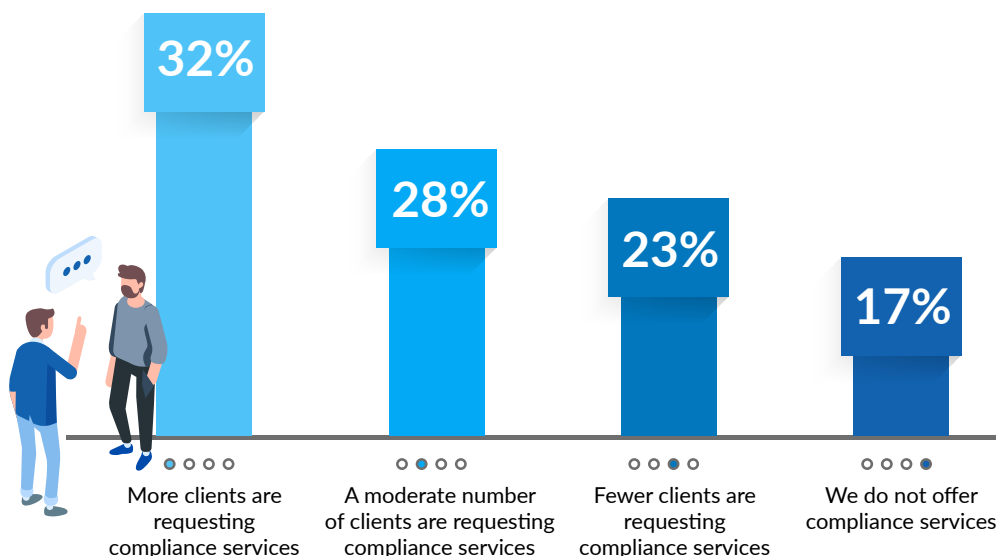
Compliance Requirements of Customers

As in years past, HIPAA impacts the most survey participants (about 68 percent), followed by PCI DSS (58 percent) and GDPR (35 percent).

● 2019   ● 2018

	HIPAA	PCI DSS	GDPR	NIST	SOX	FINRA	CJIS	FERPA	Other
2019	68%	58%	35%	30%	23%	14%	7%	5%	12%
2018	55%	49%	48%	18%	27%	11%	6%	6%	11%
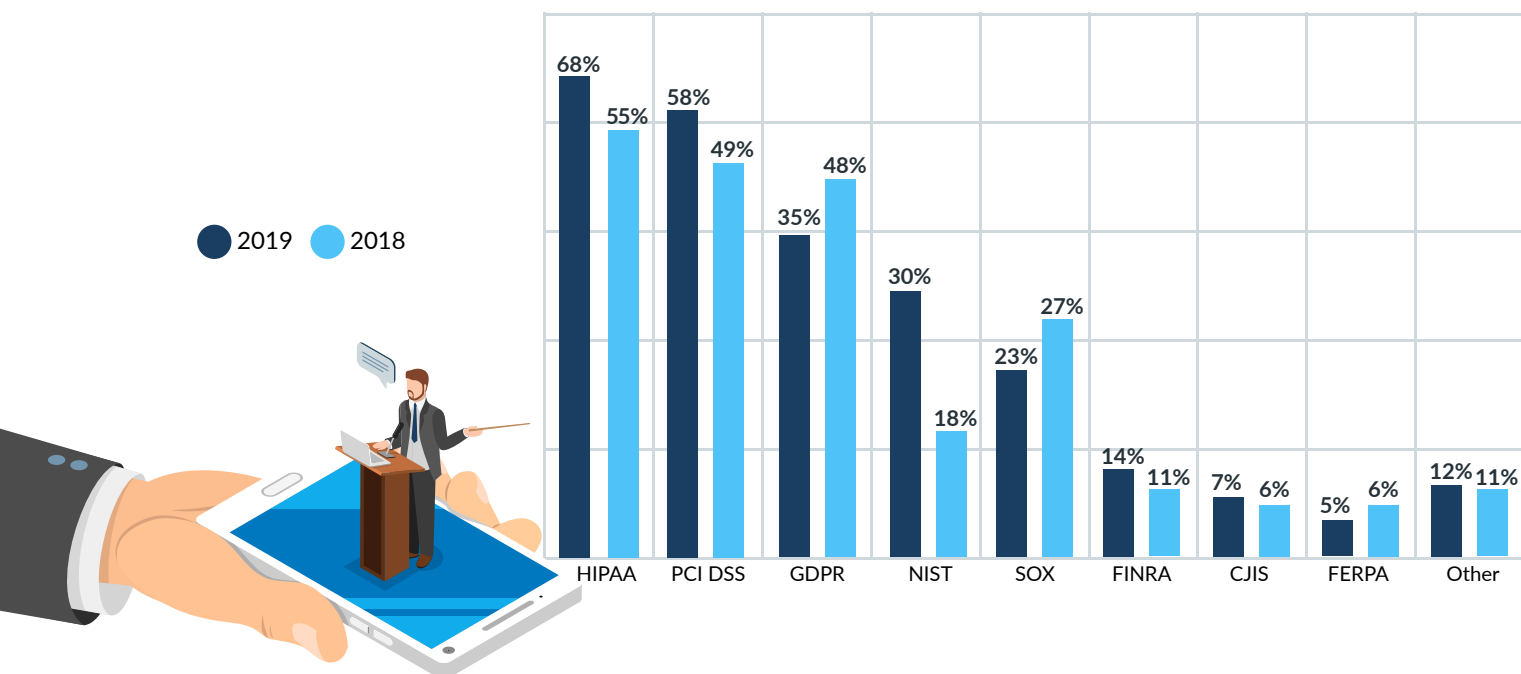
Compliance Challenges for MSPs

When asked about the regulations that respondents found difficult to comply with, most MSPs (about 31 percent) selected HIPAA, while about 23 percent selected GDPR.

As expected, in the EMEA region, GDPR took the top spot, with 59 percent of the EMEA participants finding it the most difficult to comply with.

Regulations difficult to comply with	Americas	APAC	EMEA	All Respondents
HIPAA	39%	13%	6%	31%
GDPR	14%	26%	59%	23%
PCI DSS	14%	18%	15%	14%
NIST	11%	6%	3%	9%
SOX	5%	7%	3%	5%
FINRA	4%	1%	3%	3%
CJIS	2%	1%	0%	2%
FERPA	1%	1%	0%	1%
Other	10%	25%	12%	12%

When asked if the participants ensure that their own MSP is compliant prior to rolling out a compliance service, 83 percent of them responded "Yes."

California Consumer Privacy Act

The California Consumer Privacy Act (CCPA), which went into effect on January 1, 2020, created new consumer rights relating to the access, deletion, and sharing of personal information collected by businesses.

The Act allows any California consumer to view information that any business has acquired of them. The Act gives them the right to opt out of the sale of personal information and to delete the information held by businesses.

The CCPA applies to businesses that:
• Have gross annual revenue in excess of $25 million
• Buy, receive or sell personal information of 50,000 or more consumers
• Derive 50 percent or more of their annual revenue through the sale of consumers' personal information[2]

As a result, MSPs must have a security program in place to protect their customers and comply with the CCPA regulation. However, not many MSPs are informed about CCPA yet. Only 6 percent of all respondents said they were "very informed" about the CCPA, while 23 percent said they were "somewhat informed" regarding the legislation.

Familiarity With CCPA

6%	23%	36%	35%
Very informed	Somewhat informed	Not very informed	Completely uninformed
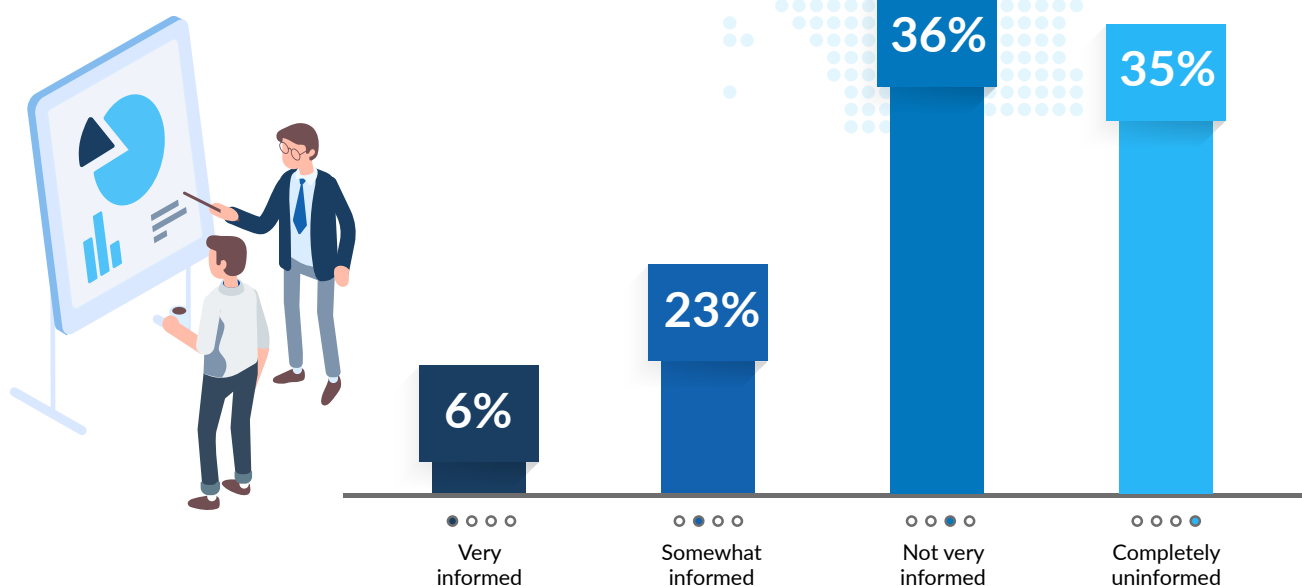
Managed Services Represent a Significant Percentage of the Revenue for MSPs

MSPs have undergone a tremendous evolutionary shift over the past decade. From break-fix services to providing full-fledged suites of services, and negotiating subscription contracts to reselling software, MSPs have become quite sophisticated in managing their clients' IT operations.

Today, managed services represent an average of about 30 percent of the revenue for all MSPs. Hardware and software resale represents nearly 17 percent of the revenue, whereas break-fix services represent a mere 13 percent.

Service Category	2019 Average Percentage of Revenue	2018 Average Percentage of Revenue
Managed services	30%	32%
Hardware or software resale	17%	16%
Break-fix services (based on hourly, block hours or staff augmentation)	13%	15%
Professional (project) services	13%	14%
Backup and disaster recovery services	6%	NA
Software sales (your own software)	5%	6%
Private cloud services (hosting client infrastructure)	4%	4%
Enhanced security services (e.g., 2FA, IDS/IPS, and penetration testing)	3%	2%
Public cloud services (managing client infrastructure in public clouds e.g., Azure, AWS, Google, IBM, US Signal, Rackspace, Pax8)	3%	3%
Compliance assessment services	2%	2%
DevOps (delivering applications)	1%	1%
Other	2%	4%

Managed Services Provided

Managed Services Provided	2019	2018
Help desk/desktop support	88%	93%
Network and connectivity support	83%	91%
Server support	83%	91%
Antivirus/anti-malware	81%	86%
Backup and recovery (either cloud or onsite)	81%	82%
Remote monitoring	80%	83%
Patching and updates	79%	84%
Office 365 management	74%	75%
Managed firewall	72%	70%
Third-party software patching and updates	62%	63%
Client assessment	61%	60%
Enhanced network performance monitoring/infrastructure availability	60%	61%
Audit and discovery	59%	63%
Office 365 backup	56%	48%
Intrusion detection and prevention (IDS/IPS)	54%	46%
Cloud services (e.g., IaaS, PaaS, SaaS)	53%	52%
Identity & access management security (e.g., 2FA, SSO, and password management)	50%	45%
Cloud monitoring	43%	42%
Cloud application user/access/content management	43%	40%
Hosting services (customer-owned equipment)	40%	43%
Dark Web security monitoring	32%	15%

The managed services that bring in the highest growth in MRR for MSPs are network and connectivity support, RMM, server support and antivirus/antimalware protection.

Managed Services   Average growth of MRR>20%

▶▶ **Network and connectivity support**   **18%**

▶▶ **Remote monitoring**   **18%**

▶▶ **Server support**   **18%**

▶▶ **Antivirus/antimalware**   **18%**

This year's survey also saw an increase in the number of respondents providing managed services, like Office 365 backup (an 8 percent increase), intrusion detection and prevention (also an 8 percent increase), identity and access management security (5 percent increase) and Dark Web security monitoring (a whopping 17 percent increase).

Managed services	2019	2018
Office 365 backup	56%	48%
Intrusion detection and prevention (IDS/IPS)	54%	46%
Cloud services (e.g., IaaS, PaaS, SaaS)	53%	52%
Identity & access management security (e.g., 2FA, SS0, and password management)	50%	45%
Cloud monitoring	43%	42%
Cloud application user/access/content management	43%	40%
Dark Web security monitoring	32%	15%
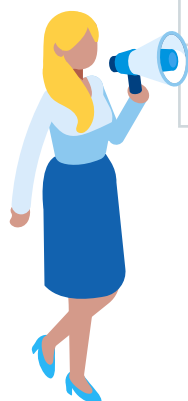
Network Monitoring and Management Services Offered

IT departments in small businesses are finding it highly challenging to manage their networks. They are turning to MSPs to keep their businesses running smoothly and protect them from costly downtime. Although network monitoring and management is one of the basic services provided by MSPs, it is a huge responsibility since it includes configuration management, performance management and security management, all of which are required for the functioning of IT infrastructure. One of the core features of network monitoring includes real-time visibility (not an option anymore), which enables MSPs to identify and troubleshoot issues in the network and keep IT running.

Network Monitoring and Management Services Offered

LAN/WAN	Onsite, physical devices	Onsite, virtual devices	Public cloud (customer licensed)
82% 90% 85%	78% 88% 84%	68% 73% 68%	37% 41% 42%

Public cloud (MSP licensed)	Private cloud (customer-owned equipment)	Private cloud (MSP-owned equipment)	Hybrid cloud
42% 45% 45%	38% 39% 41%	36% 42% 45%	37% 40% 41%

We do not provide network monitoring
6% 0% 0%

2019 2018 2017
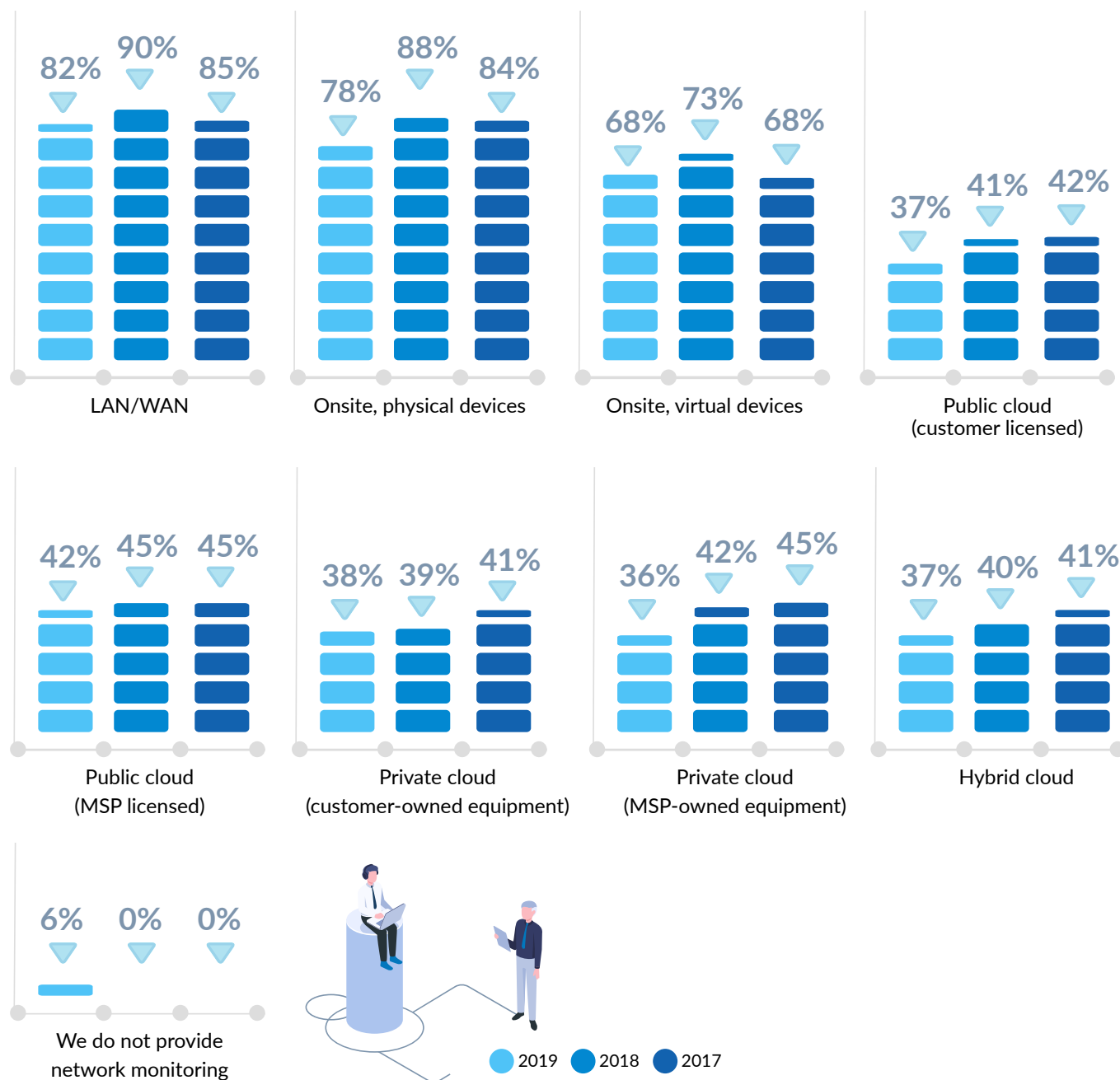
BACKUP AND RECOVERY

## Onsite-to-Cloud Backup Method Remains at the Top for All Regions

Almost all respondents (about 97 percent) provide some or the other kind of backup service, while about 61 percent of respondents implement onsite-to-cloud backup as the primary backup method for their client data.

Backup Method Used	Americas	APAC	EMEA	All Respondents
Onsite-to-cloud backup	64%	47%	54%	61%
Onsite-to-onsite backup	11%	25%	18%	14%
Appliance-based backup infrastructure	13%	12%	10%	12%
Cloud-to-cloud backup	5%	9%	9%	6%
Cloud-to-onsite backup	3%	0%	3%	2%
SDN-based backup	1%	3%	0%	1%
We do not provide backup services	3%	4%	6%	4%

SaaS Backup for Customers

More than half the respondents (53 percent) currently back up their clients' SaaS applications, such as Office 365, G Suite and Salesforce.
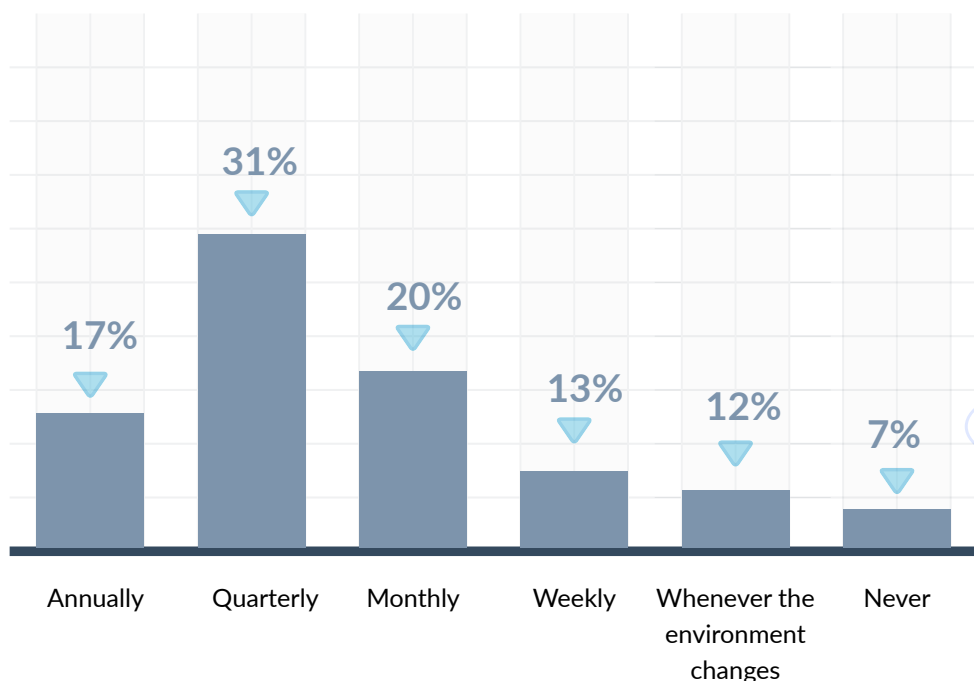
MSPs That Back Up Customers' SaaS Applications

YES
53%
44%

NO
47%
56%

★ 2018   ★ 2019
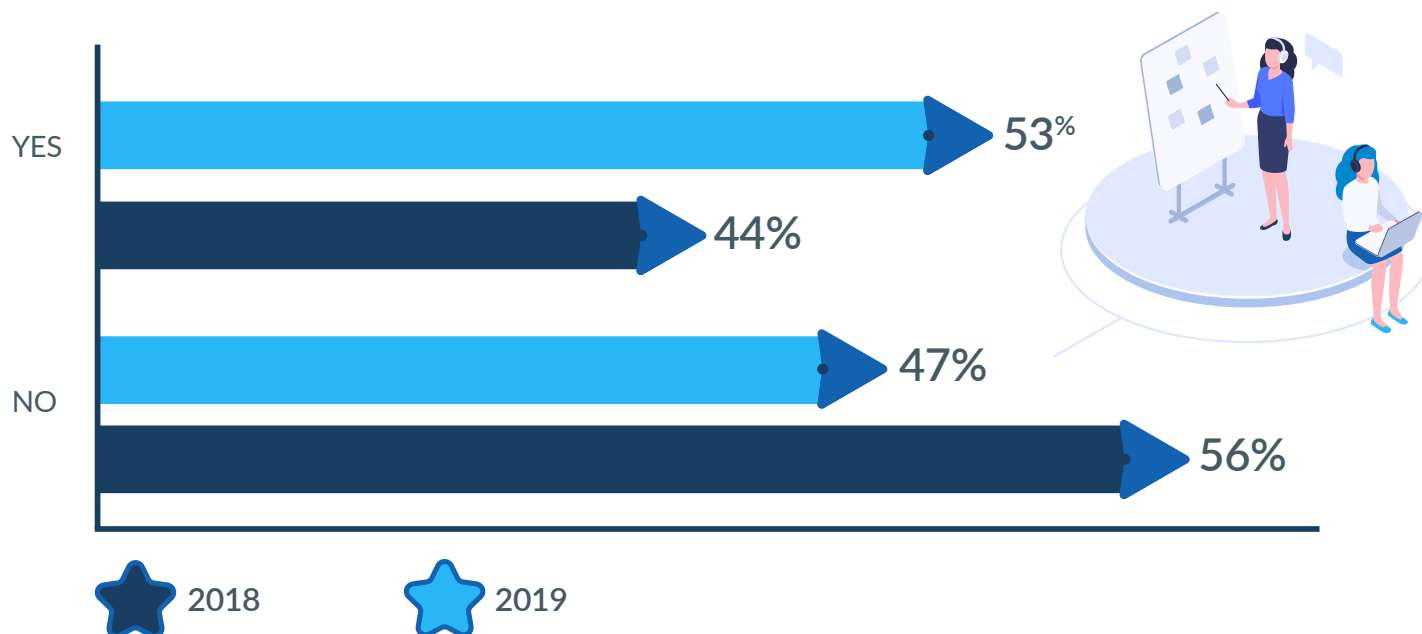
Client Data Recovery Testing

Only about half (48 percent) of respondents test their clients' recovery capabilities quarterly or annually. This is too infrequent to provide strong confidence in the recoverability of their data.

The Regularity of MSPs Testing Their Clients' Recovery Capabilities

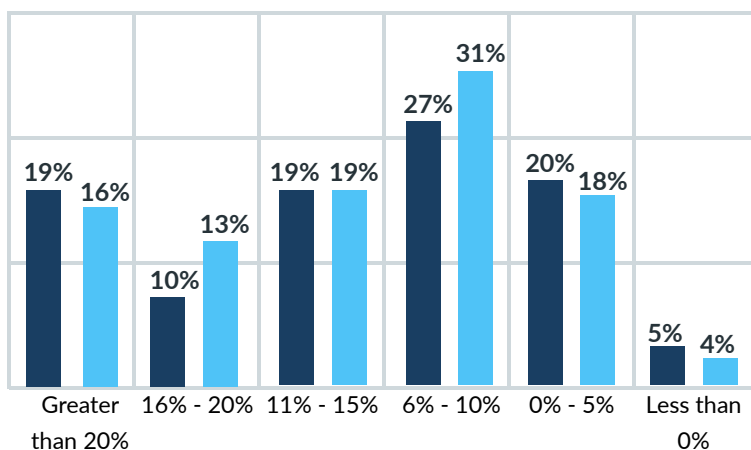| Category	Percentage
Annually	17%
Quarterly	31%
Monthly	20%
Weekly	13%
Whenever the environment changes	12%
Never	7%

MSP GROWTH AND PRICING STRATEGY

Monthly recurring revenue is a key component of the MSP business model that every MSP that isn't providing only break-fix services monitors. When asked about their MRR growth, only 19 percent of respondents said they experienced an average growth greater than 20 percent over the past three years. Another 27 percent experienced an average MRR growth ranging between 6 to 10 percent.

Average Year-Over-Year Growth of MRR

● 2019 ● 2018

Range	2019	2018
Greater than 20%	19%	16%
16% - 20%	10%	13%
11% - 15%	19%	19%
6% - 10%	27%	31%
0% - 5%	20%	18%
Less than 0%	5%	4%

This year, same as last year, more respondents opted for a value-based pricing strategy rather than cost-based or price-match strategies.

Of all the respondents, 38 percent get more than 50 percent of their revenue from a value-based pricing strategy.

Of all the respondents, 17 percent get more than 50 percent of their revenue from a cost-based pricing strategy.

Pricing Strategy	0%	1 - 10%	11 - 20%	21 - 30%	31 - 40%	41 - 50%	More than 50%
Price-match	50%	21%	13%	8%	3%	3%	3%
Cost-based (cost of goods sold + fixed margin)	15%	7%	15%	13%	14%	18%	17%
Value-based (price based on delivered result and value delivered to the customer)	11%	7%	8%	8%	10%	18%	38%

High Growth Margins With Value-Based Pricing

Pricing can be tricky for MSPs. They must maintain a balance between pricing their services competitively and maintaining healthy gross margins that allow them to grow their business. As per our survey, high-growth MSPs favor value-based pricing over cost-based and price-match pricing.

Among our high-growth respondents, 53 percent (who have an average MRR growth greater than 20 percent) get more than 50 percent of their revenue from value-based pricing.

Percentage of total revenue	Price-match	Value-based	Cost-based
0%	58%	9%	13%
1 - 10%	23%	3%	9%
11 - 20%	8%	3%	15%
21 - 30%	4%	6%	15%
31 - 40%	5%	6%	12%
41 - 50%	2%	20%	18%
More than 50%	2%	53%	18%

Pricing Model – Per-User, Per-Device and Per-Hour

The per-user pricing model seems to be the most popular among respondents.

Of the respondents, 26 percent charge more than 50 percent of their total customer base on a per-user pricing basis.

Of the respondents, 24 percent charge more than 50 percent of their total customer base on a per-device pricing basis.

Of the respondents, 14 percent charge more than 50 percent of their total customer base on a per-hour pricing basis.

Percentage of total customer base	Per-user	Per-device	Per-hour
0%	22%	19%	19%
1 - 10%	11%	10%	24%
11 - 20%	10%	10%	14%
21 - 30%	12%	10%	10%
31 - 40%	7%	8%	8%
41 - 50%	12%	18%	11%
More than 50%	26%	24%	14%

APPENDIX

Additional Pricing Data

Most frequently quoted hourly rate

● 2019 ● 2018

	Up to $50/hour	$51 - $100/hour	$101 - $200/hour	$201 - $250/hour	More than $250/hour	We don't have an hourly rate option
2019	5%	17%	65%	5%	1%	6%
2018	11%	21%	64%	2%	2%	0%
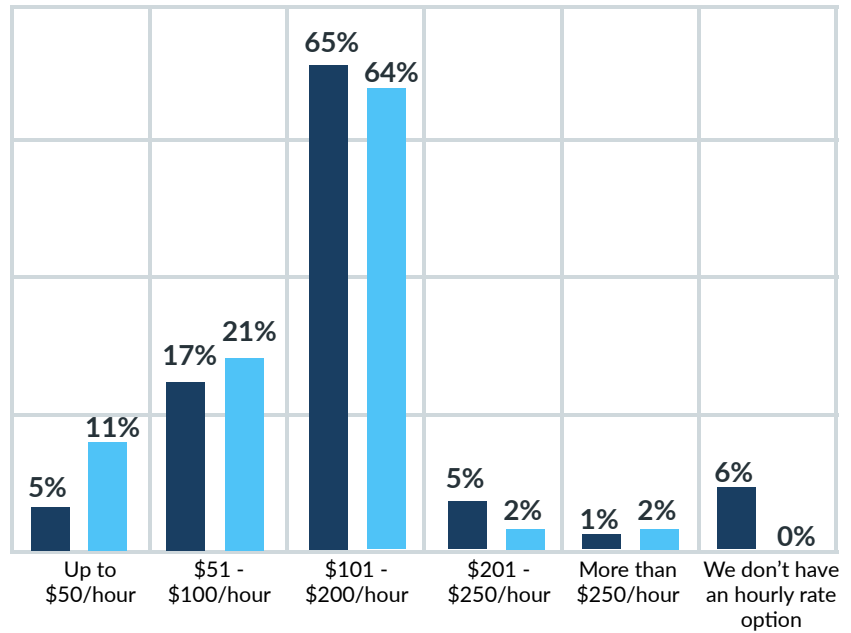
Most frequently quoted standard hourly rate	Americas	APAC	EMEA	All Respondents
Up to $50/hour	2%	11%	18%	5%
$51 - $100/hour	13%	15%	46%	17%
$101 - $200/hour	73%	55%	27%	65%
$201 - $250/hour	6%	2%	2%	5%
More than $250/hour	1%	2%	1%	1%
We don't have an hourly rate option	5%	15%	6%	6%

Average size of monthly managed services contract

● 2019   ● 2018

Category	2019	2018
Less than $1,000	22%	17%
$1,001 - $2,500	30%	27%
$2,501 - $5,000	20%	26%
$5,001 - $7,500	7%	9%
$7,501 - $10,000	4%	4%
More than $10,000	4%	8%
Not applicable	13%	
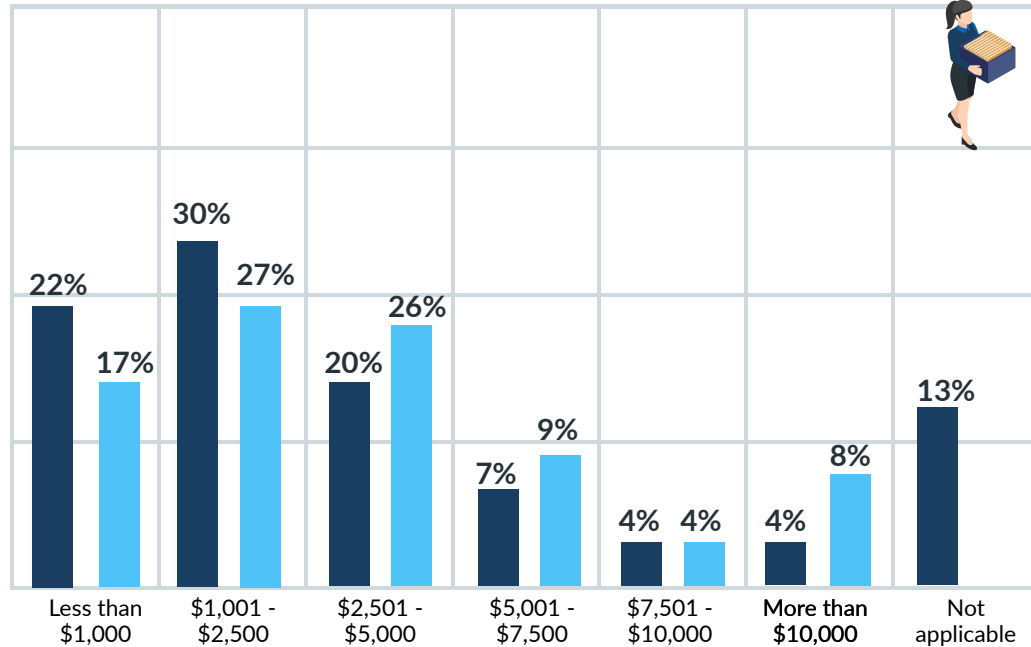
Average size of monthly managed services contract	Americas	APAC	EMEA	All Respondents
Less than $1,000	20%	16%	31%	22%
$1,001 - $2,500	31%	32%	24%	30%
$2,501 - $5,000	23%	16%	13%	20%
$5,001 - $7,500	7%	4%	8%	7%
$7,501 - $10,000	4%	3%	3%	4%
More than $10,000	3%	6%	6%	4%
Not applicable	12%	22%	15%	13%

Margin range for cloud services

Chart data:

Margin range	2019	2018
< 5%	8%	8%
6% - 10%	13%	15%
11% - 20%	23%	25%
21% - 30%	17%	17%
31% - 40%	9%	10%
41% - 50%	3%	6%
More than 50%	6%	6%
We do not offer cloud services at this time	21%	13%

● 2019   ● 2018
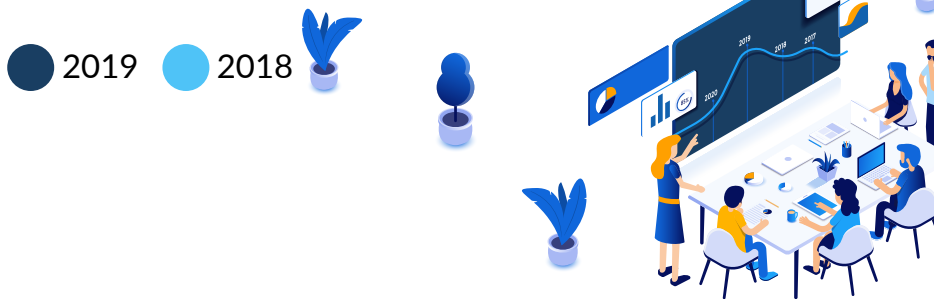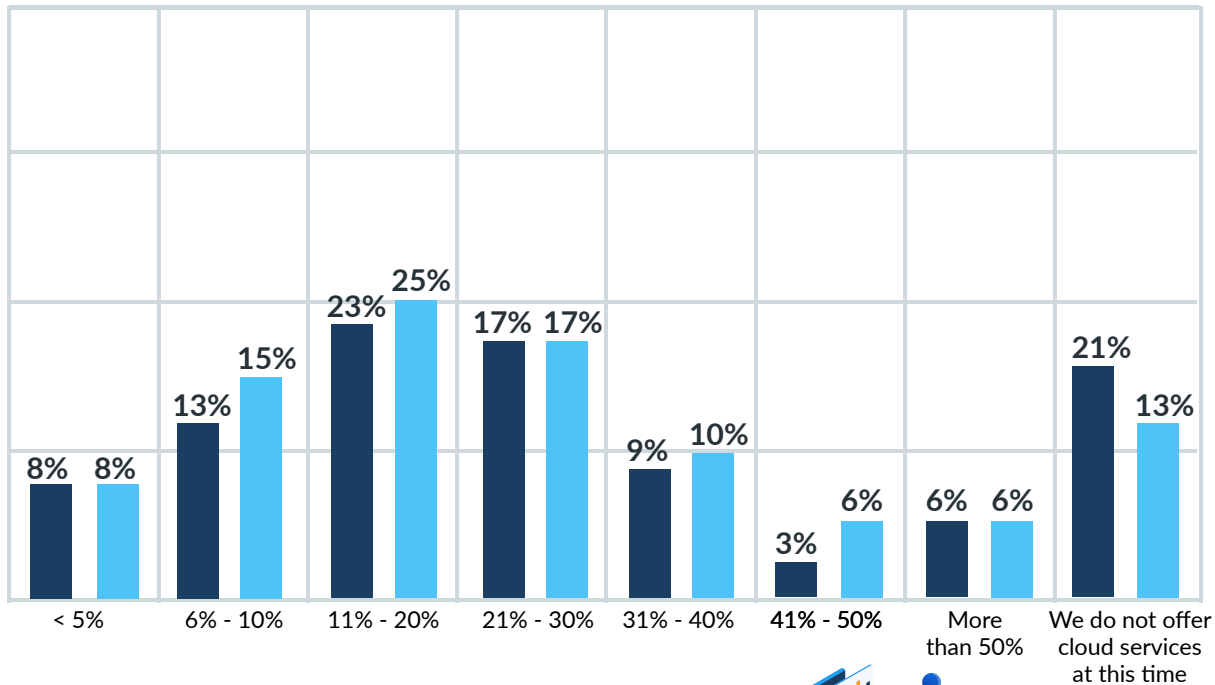
Margin range for cloud services	Americas	APAC	EMEA	All Respondents
< 5%	8%	9%	6%	8%
6% - 10%	11%	21%	18%	13%
11% - 20%	24%	19%	18%	23%
21% - 30%	16%	23%	20%	17%
31% - 40%	9%	9%	12%	9%
41% - 50%	4%	2%	2%	3%
More than 50%	6%	9%	7%	6%
We do not offer cloud services currently	23%	9%	18%	21%

Average charge per device, per month, for ongoing server support and maintenance

● 2019   ● 2018
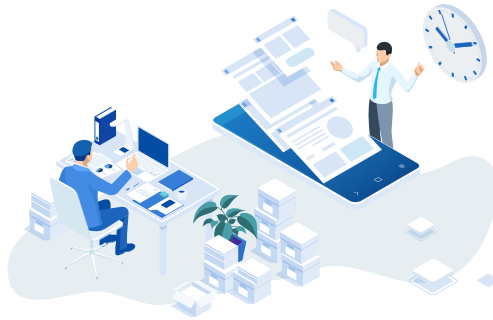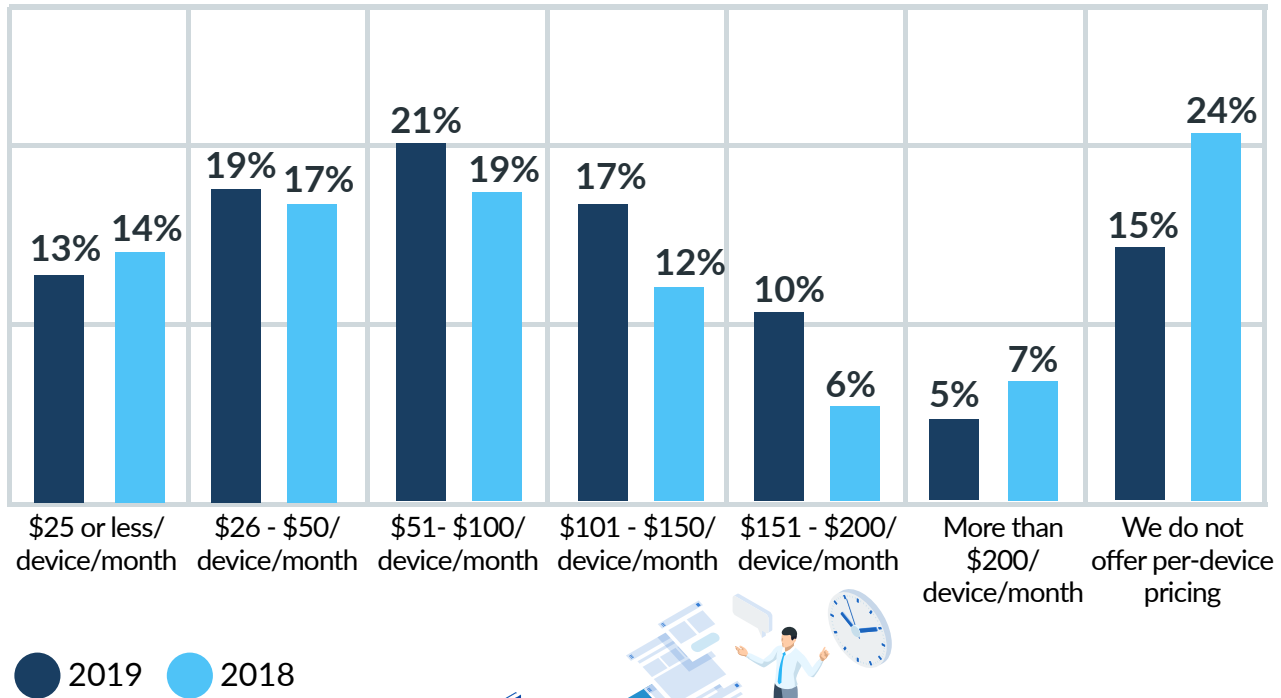
Average charge per device, per month for ongoing server support and maintenance	Americas	APAC	EMEA	All Respondents
$25 or less/device/month	9%	32%	24%	13%
$26 - $50/device/month	19%	17%	24%	19%
$51- $100/device/month	21%	21%	21%	21%
$101 - $150/device/month	18%	11%	13%	17%
$151 - $200/device/month	11%	4%	5%	10%
More than $200/device/month	6%	0%	0%	5%
We do not offer per-device pricing	16%	15%	14%	15%

Charges for cloud monitoring services per month

Legend: ● 2019 ● 2018
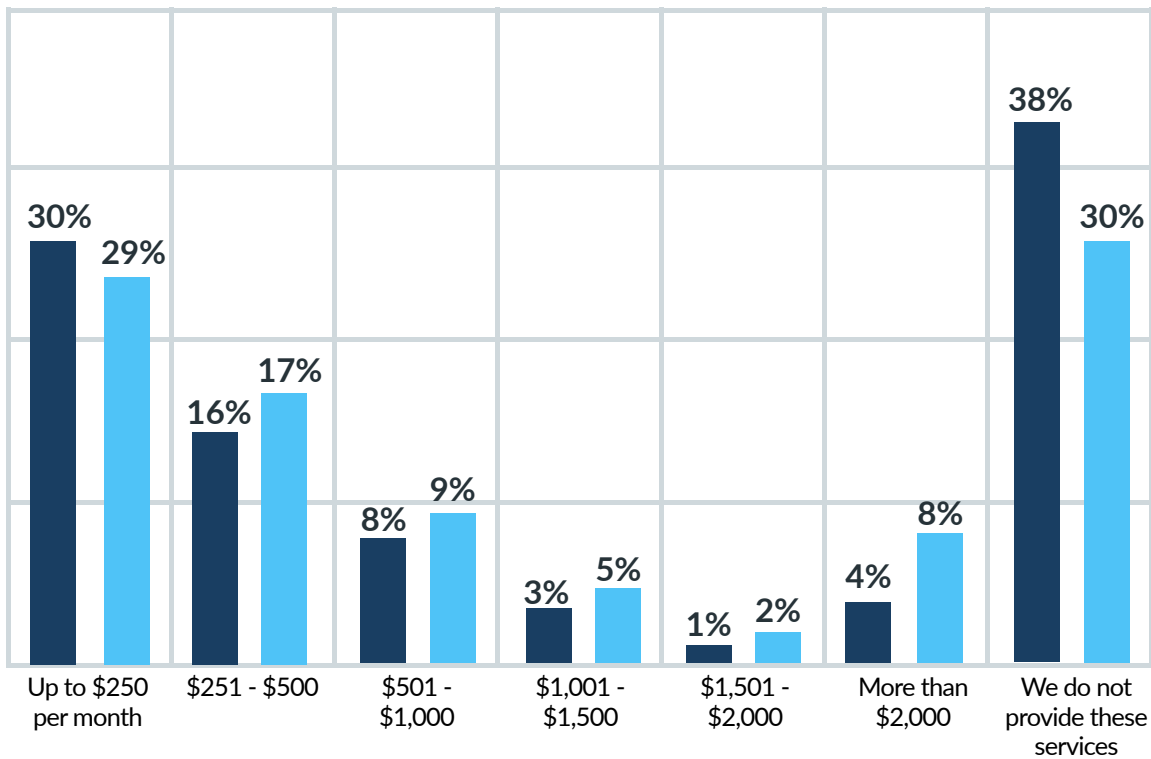
Chart values by category:
- Up to $250 per month: 30% (2019), 29% (2018)
- $251 - $500: 16% (2019), 17% (2018)
- $501 - $1,000: 8% (2019), 9% (2018)
- $1,001 - $1,500: 3% (2019), 5% (2018)
- $1,501 - $2,000: 1% (2019), 2% (2018)
- More than $2,000: 4% (2019), 8% (2018)
- We do not provide these services: 38% (2019), 30% (2018)

Charge per month for cloud monitoring services	Americas	APAC	EMEA	All Respondents
Up to $250 per month	28%	34%	37%	30%
$251 - $500	16%	18%	15%	16%
$501 - $1,000	8%	6%	8%	8%
$1,001 - $1,500	4%	1%	1%	3%
$1,501 - $2,000	2%	1%	1%	1%
More than $2,000	4%	3%	3%	4%
We do not provide these services	39%	37%	35%	38%

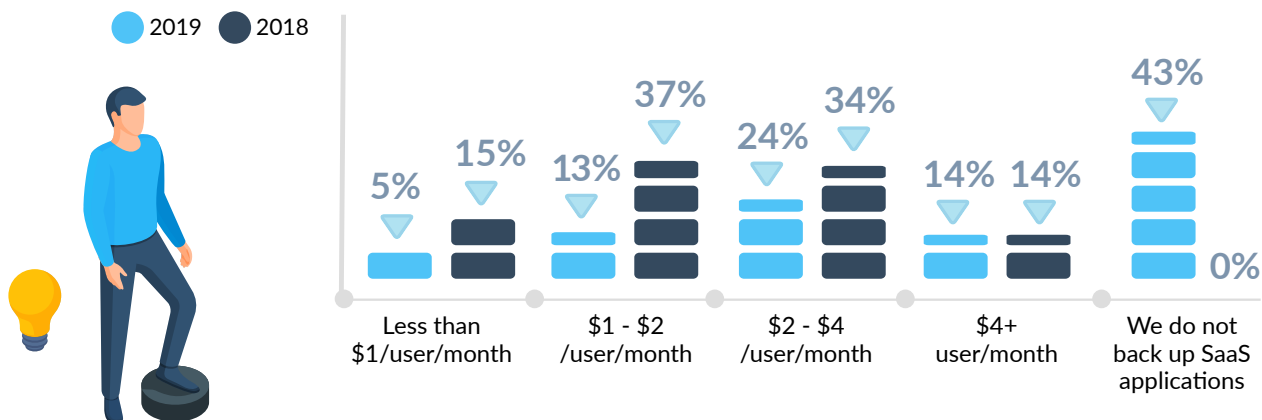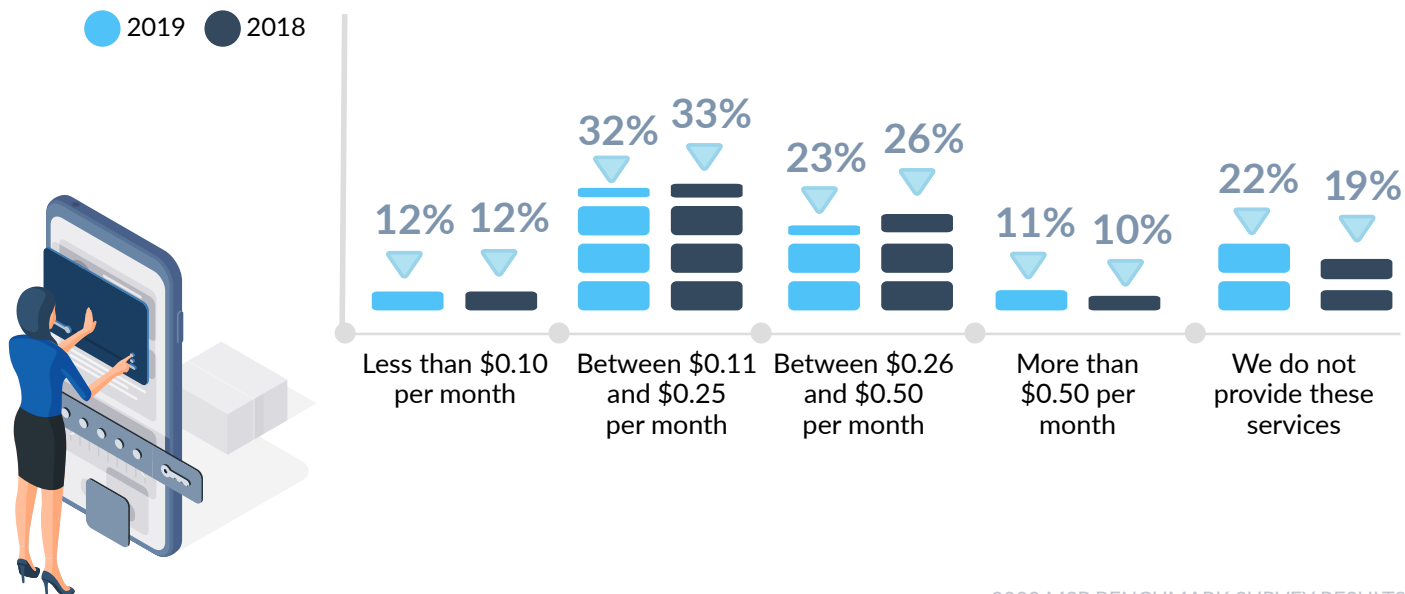## Charge per user, per month for ongoing user support — e.g., help desk and end-user device management
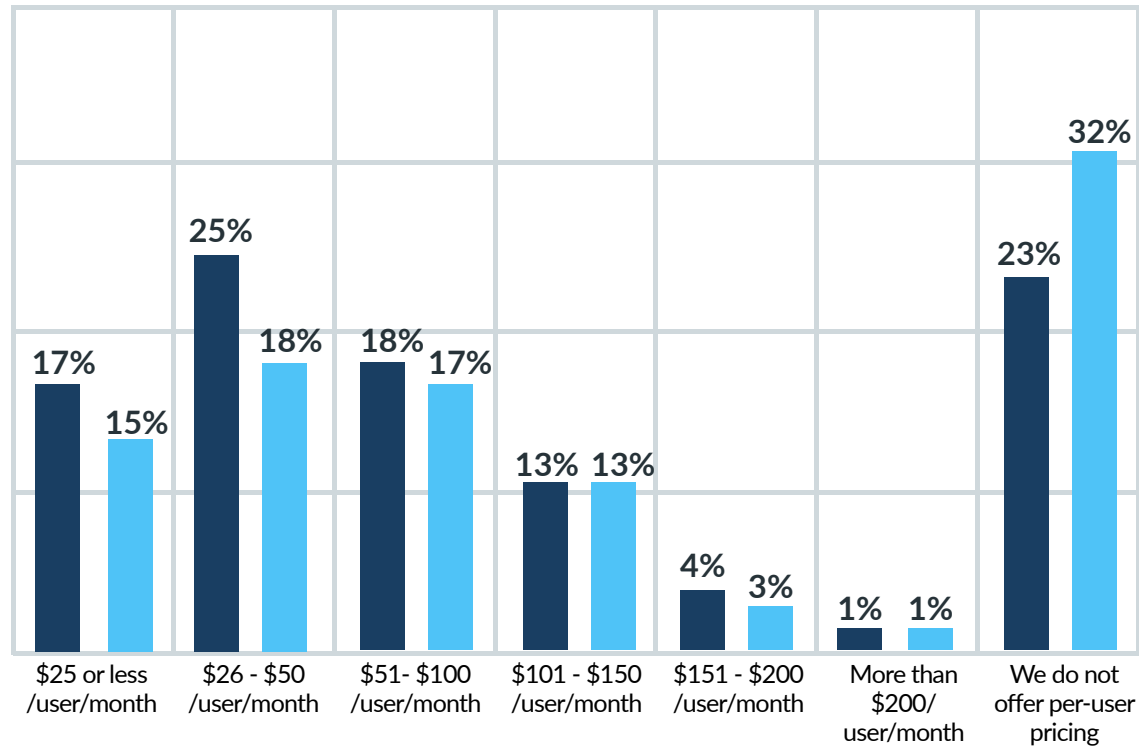
2019 **2018**
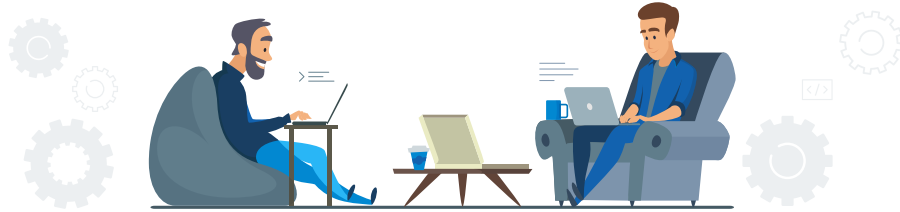
Charge per user, per month for ongoing user support	Americas	APAC	EMEA	All Respondents
$25 or less/user/month	12%	28%	31%	17%
$26 - $50/user/month	25%	16%	31%	25%
$51- $100/user/month	21%	15%	12%	18%
$101 - $150/user/month	15%	9%	4%	13%
$151 - $200/user/month	4%	1%	1%	4%
More than $200/user/month	1%	0%	0%	1%
We do not offer per-user pricing	22%	31%	22%	23%

Charge per user, per month to back up customers' SaaS applications

● 2019 ● 2018

	Less than $1/user/month	$1 - $2 /user/month	$2 - $4 /user/month	$4+ user/month	We do not back up SaaS applications
2019	5%	13%	24%	14%	43%
2018	15%	37%	34%	14%	0%

How much do you charge per user, per month to back up your customers' SaaS applications?	Americas	APAC	EMEA	All Respondents
Less than $1/user/month	4%	7%	6%	5%
$1 - $2/user/month	12%	10%	21%	13%
$2 - $4/user/month	26%	24%	19%	24%
$4+ user/month	15%	18%	8%	14%
We do not back up SaaS applications	43%	41%	46%	43%

Charge per GB for cloud backup and recovery services

● 2019 ● 2018

	Less than $0.10 per month	Between $0.11 and $0.25 per month	Between $0.26 and $0.50 per month	More than $0.50 per month	We do not provide these services
2019	12%	32%	23%	11%	22%
2018	12%	33%	26%	10%	19%

Charge per GB for cloud backup and recovery services	Americas	APAC	EMEA	All Respondents
Less than $0.10 per month	12%	6%	12%	12%
Between $0.11 and $0.25 per month	33%	30%	28%	32%
Between $0.26 and $0.50 per month	23%	28%	21%	23%
More than $0.50 per month	11%	6%	14%	11%
We do not provide these services	20%	30%	25%	22%

Percentage of customers represented by different terms of contracts

Percentage of customer base	Less than 1 year	1 year	Between 1 year and 2 years	Between 2 years and 3 years	More than 3 years
0%	42%	26%	41%	43%	53%
1 - 10%	26%	17%	14%	10%	8%
11-20%	9%	16%	15%	8%	5%
21-30%	4%	8%	12%	13%	5%
31-40%	2%	5%	6%	9%	6%
41-50%	3%	8%	6%	7%	5%
More than 50%	14%	20%	6%	10%	18%

CONCLUSION

The MSP market's growth doesn't seem to be slowing down anytime soon. More and more MSPs are looking to grow organically by adding differentiated services to their portfolio rather than by partnering with other businesses or acquiring much smaller businesses. Security, not surprisingly, seems to be a key revenue-driving aspect, with compliance being another significant opportunity. While cloud support may take a backseat for now, it is still a viable option for MSPs to capitalize on. MSPs have finally grasped the importance of cohesive applications and have no qualms leveraging its benefits to drive better profit margins.

Survey Methodology

Kaseya conducted its annual MSP Benchmark Survey in December 2019 using structured questionnaires. Hence, as the information provided was prior to the COVID-19 pandemic, it is subject to change. To simplify the questionnaires, pricing and revenue information was requested in U.S. dollars and respondents were asked to select from price ranges rather than to specify exact figures.

To provide an indication of trends, the report includes comparable results from 2017 and 2018 where applicable. Results have been broken down by region where responses differ significantly across geographic areas. All results are included in the global statistics described as '2019'.

Overall, we've made every attempt to provide the data in a format that is most useful to the widest audience possible. Note that several questions include intentionally generalized data, given that the replies are highly variable (e.g., specific services offered in per-user pricing agreements, certain service contracts offered in remote regions of the world).

REQUEST A DEMO

OR START A FREE 14-DAY TRIAL TODAY!

Sources

1. Forecast size of the managed services market worldwide from 2019 to 2025, Statista
2. California Consumer Privacy Act (CCPA), State of California Department of Justice

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.