CONNECTWISE

CONNECTWISE EBOOK SERIES

Untapped Potential: MSPs and the SMB Market 2026 Outlook

The SMB Opportunity for MSPs: 2021–2026

Contents

Introduction: MSPs, This is Your Moment

As IT usage grows in scope and complexity, small- and medium-sized businesses (SMBs) are turning to managed services providers (MSPs) to help architect, secure, monitor, remediate, and refresh their mission-critical technology solutions so that they can deliver optimal customer experiences.

This is no minor trend: Research for "The SMB Opportunity for MSPs: 2021–2026" report from ConnectWise suggests that through 2026, SMBs will channel more than $90 billion in new spending into managed IT services.

To compete for market share, many MSPs are expanding their portfolios to include cybersecurity, compliance, and cloud services. However, they're also struggling to secure talent with in-demand skill sets. That has many MSPs looking to strategies like automation and outsourcing to ensure they can deliver new services.

This report takes a closer look at the SMB market opportunity for MSPs, how MSPs can stay relevant in a rapidly changing business landscape, and what best practices can help drive MSP success.

SMBs will channel more than $90 billion in new spending into managed IT services through 2026.

8 Key Takeaways for MSPs

1. The demand outlook for MSPs is very strong. Our research finds that nearly half of SMBs (48%) plan to prioritize IT modernization as a key business goal.
2. Post-COVID-19 work styles will fuel IT budgets. More than half of businesses (51%) plan to implement hybrid workstyles, further boosting IT investments across multiple technology areas.
3. Cybersecurity and cloud are top business priorities. Over half of SMBs (52%) intend to enhance cybersecurity, and 30% plan to migrate more IT to the cloud.
4. Compliance is a top risk for businesses to manage. About one-third of businesses (32%) will invest in cybersecurity solutions to cover regulatory and compliance risks.
5. MSPs are expanding services to meet customers' needs. The number of MSPs offering cybersecurity and compliance solutions is expected to grow 70–80% in the next three years. The number of MSPs offering cloud and collaboration solutions is expected to increase by 40–60%.
6. MSPs are focused on expanding automation use. About 100% growth is expected over the next three years in the number of MSPs using fully integrated professional service automation (PSA) and remote monitoring and management (RMM) software.
7. Many MSPs look to expand tech teams via SOCs and NOCs. The number of MSPs using security operations centers (SOCs) and network operations centers (NOCs)/ outsourced help desks is expected to grow by about 80% and 30–50%, respectively.
8. MSPs seek to increase SOC and NOC team certifications. Forty percent of MSPs attribute their cybersecurity success to the certifications earned by their SOC and NOC staff.

Chapter 1: SMBs Foresee Revenue Growth over the Next 3 Years

SMBs are experiencing a healthy recovery in the wake of the COVID-19 pandemic despite lingering supply chain issues. In fact, many expect to see double-digit growth, on average, over the next three years. The largest firms (250–999 employees), which tend to be the most resilient, will likely see the most growth during this period: 17%.

When looking at geographic trends, SMBs in the Asia-Pacific (APAC) region anticipate a faster rate of revenue growth (13%) compared with firms in North America (10%) and Europe (7%).

Along with increasing revenue, many SMBs expect to expand their use of devices over the next three years, including PCs, servers (on-premises and cloud), mobile devices, phone systems, and video surveillance systems.

Verticals prime for MSPs to target.

The following verticals should offer robust growth opportunities for MSPs over the next three years, according to our research for "The SMB Opportunity for MSPs: 2021–2026":

- **Banking and finance and legal:** These industry verticals are helping to support new business startups, relocations, and mergers and acquisitions (M&A) activity.
- **Healthcare:** This industry will continue to see patients return for non-COVID-19 care they put on hold during the past 18+ months.
- **Construction:** This vertical will continue growing as household ownership and relocation shifts play out with the new work-from-home environment.

Finally, MSPs should look to the technology, media and telecommunications (TMT) vertical for business opportunities. This sector is widening its embrace of the cloud and moving away from on-premises equipment and services.

While the average annual growth outlook for the next three years is 9% for TMT, MSPs should keep in mind that this vertical's shift to the cloud is growing at a much faster rate.

For more detailed survey results, see Appendix, Figures 1–4.

Chapter 2: IT Modernization a Priority for Capturing New Growth

The COVID-19 pandemic highlighted the importance of the customer experience—and the role that technology plays in delivering an outstanding one. SMBs are taking this lesson learned to heart and creating budgets for IT investments in areas they feel best support their specific businesses.

Fifty percent of the SMBs we surveyed report that improving the customer experience and customer loyalty is their top business goal and priority for the next three years. Upgrading IT systems and infrastructure ranked second at 48%—and this goal is obviously critical to SMBs achieving the first.

Our research also suggests that technology-enabled business processes are likely to see strong investment. For example, more than half of SMBs (52%) said that improving and expanding digitization of paper documents was a top objective. Enhancing collaboration between employees and offices ranked third among tech goals and priorities for the near future.

Cybersecurity and cloud to underpin future SMB IT investments.

Cybersecurity is top of mind for SMBs as they look to modernize their IT systems. Fifty-two percent of respondents cited cybersecurity as a top tech goal and priority for the next three years.

For many SMBs, a key component of modernization is shifting their IT to the cloud to create greater flexibility and business resilience. Nearly one-third (30%) of respondents report that they're planning to migrate more IT to the cloud and to external colocation data centers soon.

Importantly, the shift to the cloud and the focus on creating airtight cybersecurity make a business more competitive and capable of bouncing back quickly from adversity, while its less-prepared rivals deal with delays and downtime.

For more detailed survey results, see Appendix, Figures 5–6.

Chapter 3: Post-Pandemic Workspace Revamps to Fuel IT Spend

More than half (51%) of the SMBs surveyed for "The SMB Opportunity for MSPs: 2021–2026" report from ConnectWise say they plan to allow their employees to work from home for a few days every week. Only 7% of respondents said their company planned to shift to a 100% work-from-home model.

Many businesses are looking to remodel their office spaces, so that they're more flexible, secure, and collaborative. Thirty-one percent of SMBs said they'll make changes to support social distancing practices. Investments in digital signage, sensors, keyless entry and exit systems are also on deck for many SMBs.

Roughly one-quarter (23%) of businesses surveyed report that their revamp of post-pandemic workspaces includes installing and upgrading videoconferencing tools for employees. SMBs' IT modernization plans to bolster cybersecurity and invest more in cloud technology will also benefit the hybrid workforce model.

With more employees now able to work remotely in locations across the country, it's imperative for SMBs to provide a safe and highly functional work environment for their employees, both at home and within the office, so they can attract and retain top talent.

For more detailed survey results, see Appendix, Figure 7.

Chapter 4: 6 Primary Drivers for SMB Cybersecurity Investment

SMBs are key targets for cybercriminals because they can be steppingstones to compromising larger enterprises they supply goods and services to. SMBs also need to protect information of their own that attackers would find highly valuable, such as intellectual property and financial data.

Research for "The SMB Opportunity for MSPs: 2021–2026" report finds that malware downloaded from malicious emails or websites is the most common type of security incident that SMBs are experiencing. Many SMBs are seeing a wide variety of other attacks, as well, including:

- Unauthorized access and hacking incidents
- Theft of customer data, including credit card information
- Ransomware attacks
- Theft of critical business data and electronic files by external parties and insiders
- Attacks against industrial controls and equipment, including (IoT) devices

Security events typically result in system downtime for SMBs. Damage to PCs, servers and other hardware, which can be costly to repair, is another top impact. However, other fallout from a security incident can be much more costly and even cripple a business, such as the loss of customer trust.

Regulatory fines and penalties related to data breaches can also hurt an SMB's bottom line. In fact, compliance with regulatory and legal requirements is driving many SMBs to increase their cybersecurity investments in the near term. It ranks third among the top six reasons for making these investments:

1. Safeguarding company data, communications and intellectual property: 43%
2. Guaranteeing customers' privacy and financial data: 39%
3. Compliance with regulatory and legal requirements: 32%
4. Growth of mobile users and connectivity to the corporate network: 29%
5. Protecting physical assets and infrastructure (e.g., offices, warehouses): 28%
6. Digitalization of company business processes: 28%

For more detailed survey results, see Appendix, Figures 8–10.

Chapter 5: IT 9-1-1: More SMBs Turning to MSPs for Help

With all the IT challenges they're facing, it's not surprising that many SMBs are reaching out to external experts for help. Here are some of the main reasons these businesses need support from MSPs now more than ever:

Growing IT complexity
As SMBs pursue digital transformation, they must undertake complex integrations across legacy systems, the cloud, and multiple business processes.

Proliferation of endpoints
According to our survey, SMBs expect 25–30% growth, on average, in the number of endpoints installed over the next three years.

Lack of IT resources
Over 40% of SMBs have no internal IT staff, and most of these businesses have no more than one generalist on hand.

New work styles
The work-from-anywhere trend and the intermingling of home and office IT infrastructure require SMBs to focus more attention on security and provide remote support readiness.

Cybersecurity confusion
Many SMBs need help navigating cybersecurity technology options. Over 40% report having difficulty understanding cybersecurity and knowing what solutions to implement and how.

Worsening threat landscape
About 60% of businesses have experienced a financially damaging cyberattack in the past 12 months.

Compliance overload
Over 40% of SMBs said they don't understand how to navigate compliance regulations related to IT, which change frequently.

SMBs need dedicated help to manage compliance.

About 20–25% of SMBs surveyed said they've assigned compliance work to an external IT services provider to relieve business management of this responsibility. As more SMBs follow suit, it will be vital for MSPs to master vertical-specific compliance issues so that they can liaise effectively with their customers' senior staff on these matters.

For more detailed survey results, see Appendix, Figures 11–12.

Chapter 6: SMBs Look to Budget More for Managed IT Services

Many SMBs, recognizing that MSPs can be critical partners in helping them overcome their IT challenges, are planning to increase investment in managed IT solutions. The widespread and growing need for process digitization, cloud migration, post-COVID-19 collaboration, analytics, and better security are all creating strong demand from SMBs for external expertise in IT.

Research for "The SMB Opportunity for MSPs: 2021–2026" report suggests SMBs' investments in managed IT solutions that will help them achieve their business goals and improve ecosystem collaboration and engagement will grow at 2–3 times the rate of investments in all other IT solutions.

As budgets for managed IT services expand over time, the challenge for MSPs will be targeting SMBs that are ready and able to move quickly into the managed model and prepared to shift most of their IT budget in that direction.

Where MSPs can find opportunities to grow accounts and revenue.

SMBs will be looking to MSPs to help them strategize and prioritize digital transformation and other IT modernization projects. Many will also lean on MSPs to help them address critical knowledge gaps in compliance, security, and analytics, and to implement vertical-focused solutions.

Based on our research, we also expect to see microbusinesses that lack internal IT employees to hire MSPs as their complete IT department. Meanwhile, SMBs with internal IT will likely look to MSPs to co-manage IT and provide strategic guidance and support.

For more detailed survey results, see Appendix, Figures 13–14.

Over **80%** of all SMBs in North America, Europe and the APAC region are currently spending on managed IT services—and devoting **20%** of their annual IT budgets, on average, toward these services.

Chapter 7: Managed IT Services Spending to Spike Worldwide

Over $90 billion in new spending will be created in managed IT services between 2021 and 2026. SMBs in North America are expected to add more than $30 billion in net-new spending during that time frame.

While we anticipate that total managed services spend will grow at 14% through 2026, we see managed cybersecurity and the cloud outpacing the overall market with 18% during that same period.

The growth in this market provides immense opportunities to MSPs that can offer broad service portfolios. As SMBs expand their managed IT services spend, they will, over time, seek out MSPs with these expanded portfolios for ease of procurement and relationship management.

However, as the next chapter explains, MSPs that want to benefit from this emerging boom time in managed IT services spending around the globe will need to level up to meet businesses' expectations. Otherwise, they risk missing out on capturing an immense opportunity to grow their business.

For more detailed survey results, see Appendix, Figures 15–16.

Through 2026, SMB spending on total IT will grow at a 6% CAGR. But spending on managed IT services will grow at more than 2X that rate—at a 14% CAGR.

Chapter 8: MSPs Under Pressure to Meet New Expectations

A major theme that emerged from our SMB survey for "The SMB Opportunity for MSPs: 2021–2026" report is these businesses want to work with high-quality service providers that can offer a broad range of capabilities and execute them well.

Following are the top three capabilities that business decision-makers cited as "critical" for an IT service provider to possess:

- Well-managed, and adheres to IT industry best practices: 28%
- Offers a comprehensive suite of cybersecurity solutions: 25%
- Has certified staff who are experts in a wide range of technologies and solutions: 22%

The message for MSPs is that SMBs expect IT service providers to apply leading business practices because their own business has become so highly IT-enabled. And as for cybersecurity expertise, that's quickly becoming table stakes for MSPs looking to earn the business of SMB customers. SMBs also want to collaborate with partners who can help them manage change and ensure every IT implementation supports business success and customer success.

SMBs want more from MSPs—but not necessarily the same things.

Being able to build, implement, fix or even optimize IT solutions is no longer enough for MSPs to be successful. They must bring much more to the table and understand market nuances if they want to keep, expand, and add new accounts in the SMB space.

Our research shows, for example, that compliance and business process know-how is essential for MSPs to move upmarket into larger-sized customer accounts. And businesses with 50 or more employees place higher importance on an IT service provider's ability to be strategic and business process-oriented.

For more detailed survey results, see Appendix, Figures 17–18.

Chapter 9: 6 Hurdles MSPs Face in Increasing Revenue and Profits

Even MSPs that already understand they need to align better to their customers' expectations currently face some significant hurdles in increasing their revenue and profits. Following are the six top challenges to capturing market growth identified in our MSP survey:

Accelerating recurring revenue
It takes anywhere from 4–7 years for MSPs to establish a high-performing, recurring revenue portfolio, and customer needs often evolve much more rapidly.

Attracting and retaining talent
Increasingly, MSPs are competing against global tech firms for talent, and about 20% of MSPs surveyed said they feel retaining their staff is a challenge.

Lack of differentiation and conveying business value
With more providers transforming into MSPs, service differentiation is becoming more challenging. For 25% of MSPs, it's now a key business goal.

Suboptimal sales growth and go-to-market
Lack of visibility into customer trends and needs makes it difficult for 25–30% of MSPs to respond to customers' changing needs and accelerate their own sales funnel.

Scaling staff productivity
The lack of the right software tools and the use of disparate tools are undermining staff productivity for many MSPs. Over 30% of MSPs report that they're now prioritizing improvements in staff efficiency.

Increased risk and liability
Threat actors are actively targeting MSPs and their customers; this is driving about 20% of MSPs to prioritize their own cybersecurity, and about 30% of MSPs to make plans to offer cybersecurity services.

Chapter 10: MSP Challenges Vary in Intensity by Region

Research for "The SMB Opportunity for MSPs: 2021–2026" report finds that MSPs across the globe face similar business challenges, although how acutely MSPs feel those challenges varies by region. That said, MSPs across regions all cited "getting clients to create budgets" as their second most significant challenge.

Improving technician productivity with new or better PSA and RMM tools is also a core concern for MSPs across North America, Europe, and the APAC region. This finding is not surprising, given that the number and complexity of solutions needed by end customers is expanding rapidly. MSPs must meet heightened demand for services while controlling their own internal operational chaos.

We also learned from our survey that MSPs across the globe are challenged in improving their sales effectiveness for similar reasons. Complex solutions with strong business process implications require a more knowledge-based and consultative approach. But not all team members are equally up to the task of delivering on that approach, which, in turn, negatively impacts sales velocity.

For more detailed survey results, see Appendix, Figure 19.

Top Business Challenge for MSPs by Region

North America: Technician productivity improvement (40%)

Europe: Demand recovery after COVID-19 (31%)

APAC: Time needed to launch new services (38%)

Chapter 11: Cyber and Compliance Maturity a Top Goal for MSPs

Across the three main geographic regions included in our survey—North America, Europe, and APAC, we found that MSPs are all highly focused on developing their cybersecurity and compliance maturity and included that objective among their top five business goals.

Our research also found that parts of MSP markets in Europe and APAC are somewhat less mature than North America's market. Some MSPs in Europe and APAC are still helping clients move to the cloud, for example, and some report that they're still formalizing their managed services practices.

North America MSPs are most heavily focused on cybersecurity and compliance services, as the chart below shows.

	North America	Europe	Asia-Pacific
1	Technician productivity improvement – 40%	Demand recovery after COVID – 31%	Time needed to launch new services – 38%
2	Getting clients to create budgets – 39%	Getting clients to create budgets – 26%	Getting clients to create budgets – 32%
3	Time needed to launch new services – 32%	Learning about new PSA, RMM tools – 26%	Technician productivity improvement – 27%
4	Learning about new PSA, RMM tools – 32%	Increasing competition – 24%	Increasing competition – 27%
5	Increasing competition – 31%	Technician productivity improvement – 23%	Learning about new PSA, RMM tools – 26%

Chapter 12: Responding to Opportunity: Expanding Portfolios

Portfolio expansion is essential for MSPs to create "customer stickiness," which includes serving current customers optimally while also taking advantage of opportunities in a growing market. And at least through 2026, cybersecurity—including securing applications, data, and infrastructure in the cloud—appears to provide the most relevant entry point for portfolio expansion.

MSPs surveyed for "The SMB Opportunity for MSPs: 2021–2026"report cited several areas where they intend to grow their portfolios within the next 36 months. Cybersecurity services that many MSPs either plan to add or expand during this time frame include:

- Cloud applications protection and security
- Email security
- Data loss prevention
- Managed endpoint security
- Network threat monitoring and vulnerability assessments

A second layer of services expansion for many MSPs in the next 36 months, will be related to enabling collaboration and securing the ever-growing range of endpoints—PCs, audio and visual devices and screens, cell phones, tablets, and IoT-enabled equipment—for their customers.

For more detailed survey results, see Appendix, Figure 20.

Chapter 13: Responding to Opportunity: Increasing Efficiency

Many MSPs are clearly recognizing that they need to raise their efficiency game if they're going to be well-prepared to manage and pursue new business in a rapidly expanding and changing market. We learned through our research for "The SMB Opportunity for MSPs: 2021–2026" report that MSPs are either already using or planning to adopt the following business management apps and platforms:

- IT document management
- Project management
- Billing and invoicing
- Customer relationship management (CRM)
- Help desk

These applications and platform adoption plans are a clear indicator of how competitive demands are growing for MSPs.

Significant jump expected in adoption of full PSA suites.

Of particular note, triple-digit growth is anticipated in MSPs' adoption of full PSA suites (129%) over the next 36 months. This indicates that more MSPs recognize that moving away from point products to a fully integrated and comprehensive PSA suite will greatly increase their efficiency by reducing the need to switch across multiple apps.

Additionally, adoption of procurement and sourcing apps is expected to increase by 120% over the same period. The ability to access a single source of truth across integrated apps is also essential for MSPs to improve staff productivity. Equally important, it allows them to deliver improved customer experiences by increasing information accuracy and response times for their clients.

These and other investment trends we identified through our research will allow many MSPs to:

- Improve sales and marketing and customer engagement capabilities via quoting, CRM, and chat applications
- Streamline procurement and goods flow through procurement and enterprise resource planning (ERP) applications
- Invest in talent training to stay relevant and competitive as technologies continue to evolve

For more detailed survey results, see Appendix, Figure 21.

Chapter 14: Responding to Opportunity: Reducing Time to Market

Access to skilled IT talent is a major hurdle to business expansion for MSPs. That's why many of these businesses are racing to invest in outsourcing options, including SOC, NOC, and relevant talent services. These investments can help MSPs reduce their time to market when rolling out new offerings, such as cybersecurity services.

An added benefit for MSPs using external resources like SOCs and NOCs is that they can strengthen their security posture with fully trained talent co-managing their service delivery operations.

A significant shift to RMM platforms expected.

Over the next 36 months, we also expect to see a 94% increase in the number of MSPs employing RMM platforms, which can also help these businesses reduce their time to market. Platforms with broad capabilities and open APIs for industry-wide integrations—including tight integration with PSA and cybersecurity platforms—will eventually replace point products, driving strong productivity and profitability impacts.

To counter competitors following this same path, MSPs should take steps now to develop a well-thought-out internal platform and create infrastructure road maps that span a time horizon of two to three years

For more detailed survey results, see Appendix, Figure 22.

Chapter 15: Elements of Cybersecurity Success for MSPs

MSPs looking to add cybersecurity services to their portfolio of offerings, or expand the services they already provide, will want to ensure that any new offering is of high-quality and "complete" so that the MSP can deliver peace of mind to their end customer.

What does a cybersecurity offering need to include to be considered "complete"? Here's what we gleaned from the security-specialized MSPs we surveyed for "The SMB Opportunity for MSPs: 2021–2026" report:

- It must be a core cybersecurity product.
- Techicians must have ongoing and up-to-date certifications.
- Compliance monitoring must be included.
- Risk insurance must be available to customers.

Also, if an MSP has a senior management team with expertise in cybersecurity, it speaks to the solutions-architecting capabilities of the business. This expertise helps to establish credibility with clients, and when communicated during the sales process, it can earn customer confidence and help seal the deal.

For more detailed survey results, see Appendix, Figure 22.

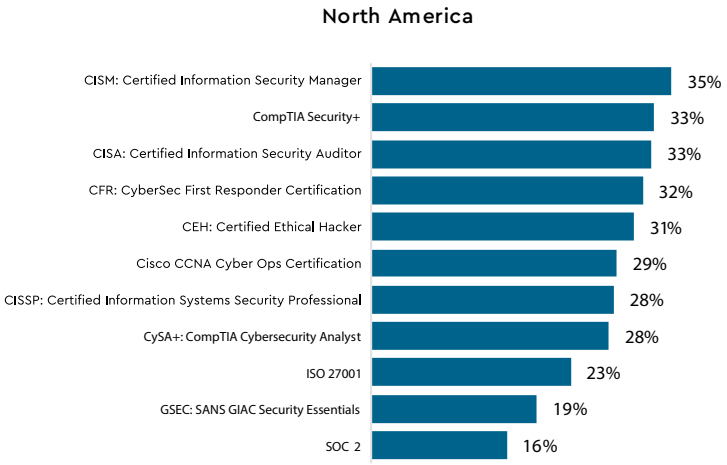
Scaling Security Services with SOC Support

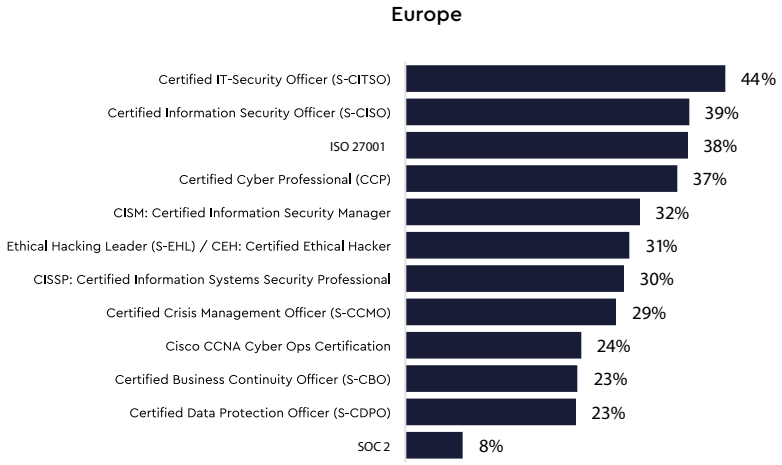
One in five security-specialized MSPs attributes the success of their business to external SOC access because it helps them add staffing volume and quality so they can scale organizational capabilities.

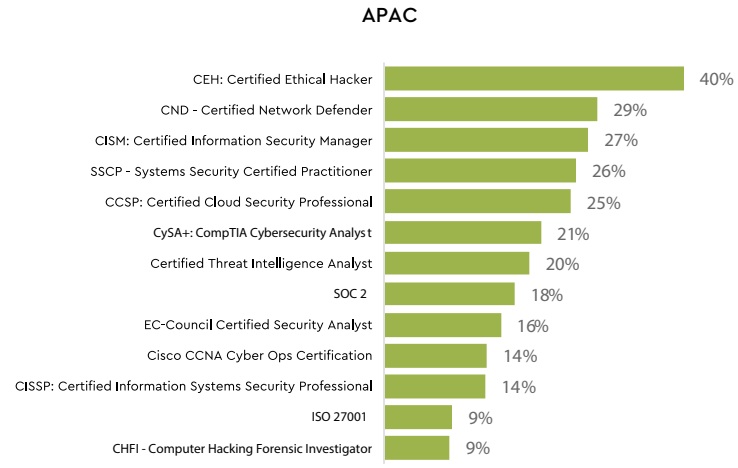
Chapter 16: The Certifications Factor

Forty percent of security-specialized MSPs surveyed for this report said that the certifications their SOC and NOC technicians possess play an essential role in the success of their managed cybersecurity services business.

Here's an overview, by geographic region, of the various cybersecurity certifications that staff across all the MSPs we surveyed presently have:







Chapter 17: MSP Operational Success Factors

The following best practices for MSP operational success are based on recommendations outlined in Service Leadership's 2021 Annual Solution Provider Industry Profitability Report™:*

1. **Have a five-year, value-creation plan.**
   What company size, revenue mix and profit do you intend to create?

2. **Have a narrowly defined target customer profile (by customer employee size).**
   This is a prerequisite to a cost-effectively narrow standard technology stack, which, in turn, enables scale, profit, a great customer experience, and strong differentiation in the marketplace.

3. **Sell your fullest suite of managed services to at least 80% of your managed services customers.**
   This approach results in the lowest sales, marketing, and general and administrative (G&A) cost per dollar of managed services revenue, among other benefits.

4. **Focus solely to decision-makers who are open to a win-win managed services arrangement.**
   These buyers are most likely to buy your fullest suite of managed services offerings, and they will let you lead on standards and pay a win-win price.

5. **Separate hunter salespeople from farmer salespeople and avoid "hybrid" hunter-farmers.**
   Pay hunters to close deals (fully managed, target customer) and move on; don't pay them on future revenue or renewals.

**Available at: service-leadership.com/solution-providers/service-leadership-index-reports/.*

Conclusions: Key Next Steps

From investing in tech talent with in-demand certifications to adopting apps and platforms that increase efficiency and enhance customer service, MSPs around the globe are now positioning to compete and thrive in a new era of managed IT services growth and opportunity.

Research shows that managed IT services providers that follow industry best practices already generate about 22% more revenue per employee compared to peers who don't adhere to these practices. They also see about 50% higher average recurring revenue (ARR) per account.

If you want your MSP business to achieve operational success in this new era, now is the time to critically assess your current offerings, practices, technology, and skillsets to ensure your business is ready to seize the moment.

For more detailed survey results, see Appendix, Figures 23.

We suggest that MSPs looking to earn their share of the growing SMB market follow these five steps:

Step 1. Consider whether the solutions you offer now will meet the needs of your customers over the next 12 to 36 months.

Step 2. Create a time-bound road map of offerings you intend to bring to customers over the next 36 months; ideally, cybersecurity should be in the mix.

Step 3. Examine whether your current tools and capabilities (and talent) will support your road map. Address any critical gaps now.

Step 4. Identify shortcomings in your customer engagement and operational practices. How could you improve your approach to differentiating your business and delighting your customers?

Step 5. Start conversations with your software providers and peer MSPs to determine how best to bridge gaps using software refreshes, outsourcing, and best practices.

Positioning your business to take full advantage of the SMB market opportunity may take time, but the potential ROI is well worth the effort. To learn how solutions from.

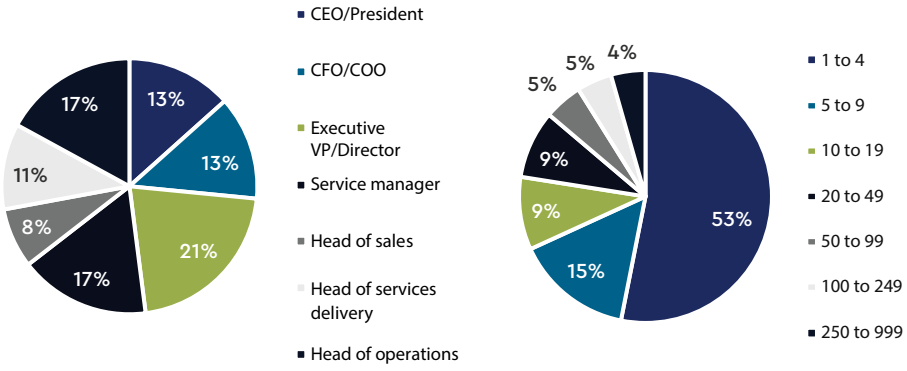
Methodology

To conduct research for "The SMB Opportunity for MSPs: 2021–2026" report, ConnectWise engaged with two leading market research firms, Analysys Mason and Hanover Research, in 1H 2021 on SMB and MSP technology needs and insights.

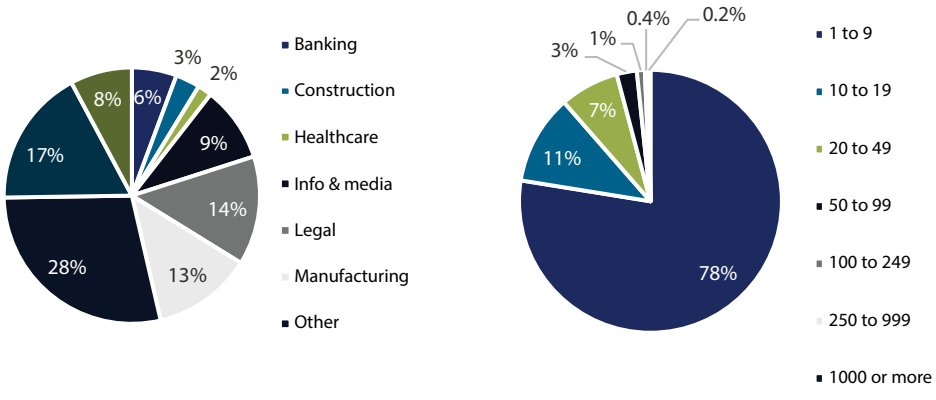
We surveyed decision-makers from about 1,000 businesses (SMBs and larger firms) and about 1,100 Technology Solution Providers (TSPs, VARs, MSPs, security-focused MSPs, office tech, and audio and visual services providers) in North America, Europe, and the Asia-Pacific region across a statistically robust representation of firm size (number of employees) and vertical industries.

"The SMB Opportunity for MSPs: 2021–2026" report used data from about 1,000 SMB surveys and a subset of about 500 MSP surveys (including security-focused MSPs). For both businesses and MSPs, we collected a statistically robust sample within employee and vertical subsegments, then weighted the data to reflect the true proportion of each subsegment within their overall populations.

MSP Respondent Profile



Business Participant Profile



Appendix: Charts and Graphics

Figure 1. Average annual revenue growth outlook for the next three years, by employee size

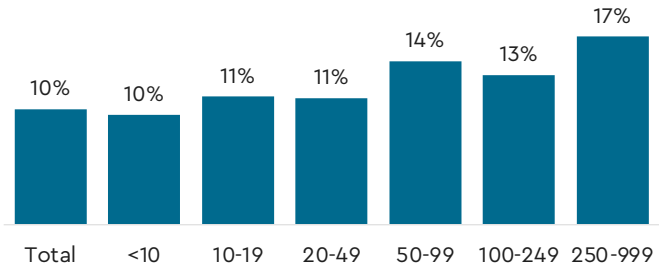


Figure 2. Average annual revenue growth outline for the next three years, by vertical

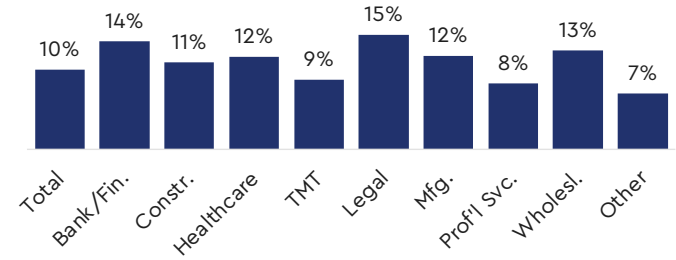


Figure 3. Annual revenue growth outlook for the next three years, by geographic region

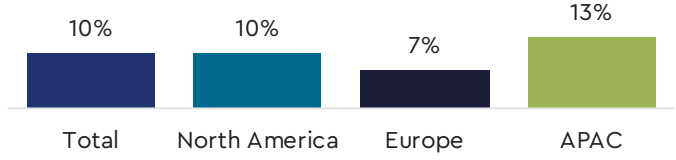
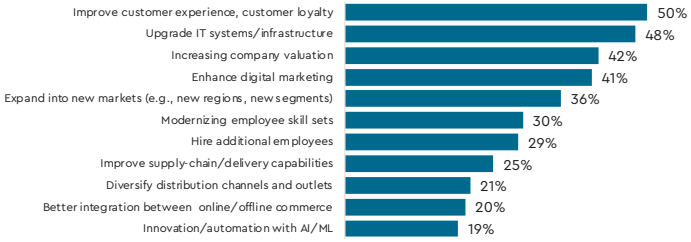


Figure 4. Device types most likely to be added over the next three years, by geographic region (% of SMBs)*

	Total	North America	Europe	APAC
PCs/laptops, including virtual desktops	65%	75%	55%	49%
Cloud servers (such as AWS, Google, Azure, etc.)	45%	43%	36%	54%
Company managed smartphones and tablets	27%	27%	24%	30%
Phone/VoIP systems	27%	27%	9%	38%
Video security/surveillance cameras	24%	22%	18%	34%
Physical/virtual servers (onsite or collocated)	19%	19%	19%	18%
Digital signage and TV screens	18%	21%	10%	15%
IoT sensors/IoT devices	16%	9%	11%	37%

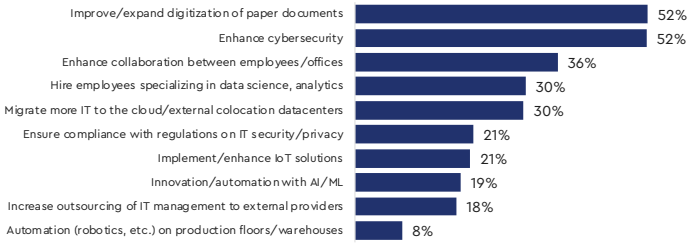
*Multiple answers allowed.

Figure 5. Business goals and priorities for the next three years (% of SMBs)*



*Multiple answers allowed.

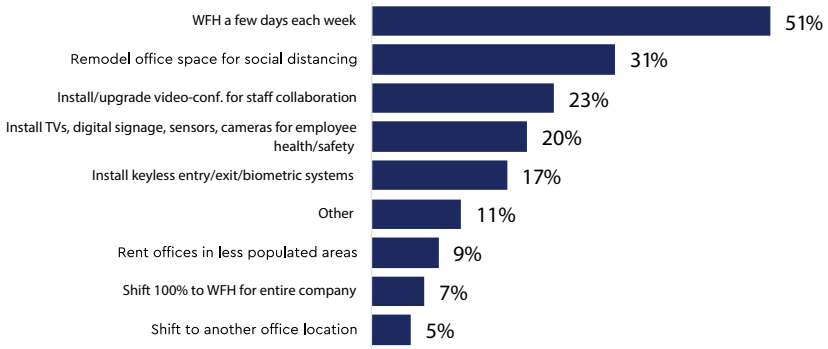
Figure 6. Technology goals and priorities for the next three years (% of SMBs)*



*Multiple answers allowed.

Appendix: Charts and Graphics

Figure 7. Workspace plans after COVID-19 pandemic (% of SMBs)*



*Multiple answers allowed.

Figure 8. Types of security incidents in the last 12 months, by geographic region (% of SMBs)*

	Total	North America	Europe	APAC
Harmful viruses or malware downloaded via emails or from websites	21%	23%	20%	16%
Denial of service attacks (DoS) that froze your website or business network	14%	9%	24%	17%
Attacks against industrial controls and equipment, including any IoT devices	12%	6%	16%	21%
Unauthorized use of company PCs, networks or mobile devices	12%	12%	4%	20%
Theft of passwords or other personal information	10%	11%	2%	11%
Impersonation of your organization's staff (phishing)	10%	7%	10%	8%
A physical break-in at your business site	9%	8%	1%	14%
Unauthorized access or hacking into your network	9%	11%	2%	10%
Theft/loss of smartphones, PCs or tablets	9%	8%	3%	16%
Theft of customers' personal or credit card information	8%	9%	2%	9%
Company systems/data locked out until payment is made (ransomware)	6%	2%	9%	15%
Theft or loss of critical business data and electronic files (from external parties or internal staff)	5%	4%	2%	10%
We did not experience any IT security-related events in the last 12 months	43%	48%	49%	24%

*Multiple answers allowed.

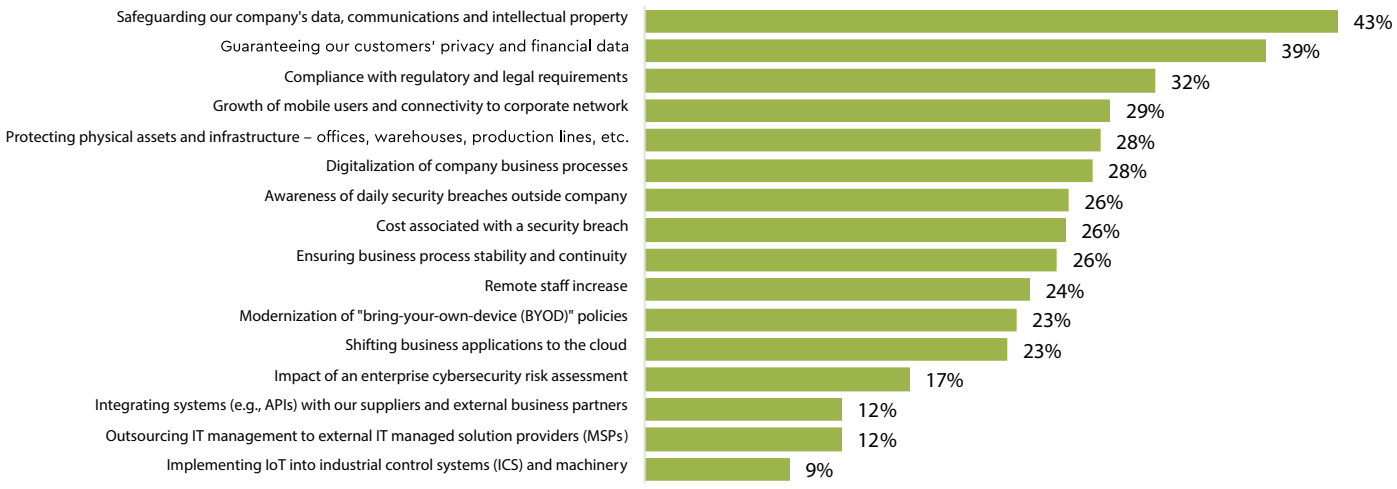
Appendix: Charts and Graphics

Figure 9. Impacts of security incidents, by geographic region (% of SMBs)*

	Total	North America	Europe	APAC
System 'downtime' and reduced productivity	29%	31%	22%	29%
Damage caused to PCs, servers, tablets or smartphones, or other hardware	18%	14%	26%	21%
Paid regulatory fines/penalties	13%	10%	14%	19%
Lost revenue	11%	10%	4%	16%
Loss of customers' trust	10%	9%	4%	19%
Loss of future business opportunities/sales	10%	8%	8%	15%
Damage to business reputation	9%	7%	3%	17%
Damage caused to other business equipment and machinery	7%	4%	3%	16%
Permanent loss of business-critical data	6%	4%	9%	7%
Lawsuits filed against our business	4%	6%	1%	3%
Fees paid to attorneys for legal matters	2%	2%	1%	2%

*Multiple answers allowed.

Figure 10. Reasons for increasing cybersecurity investments (% of SMBs)*



*Multiple answers allowed.

Appendix: Charts and Graphics

Figure 11. Key challenges with managing compliance (% of SMBs)*

	Total	North America	Europe	APAC
Complexity – difficulties in understanding regulations; we are not sure what or how to implement	38%	46%	23%	30%
Awareness – we are not sure which regulations apply to our business	31%	42%	21%	11%
Expense - Cost of implementing compliance	30%	39%	13%	21%
Staffing - Finding qualified staff to handle compliance matters	30%	29%	11%	46%
Regulatory change - Regulations change frequently, hard to stay current with changes	26%	32%	26%	12%
Regulatory expansion - The number of compliance requirements and regulations increases every year	19%	14%	33%	21%
Geographical variance - Different compliance regulations in different states/regions	17%	12%	16%	30%
Filings volume - Having to frequently file compliance certificates with regulatory authorities or business partners	16%	11%	9%	31%
Certification - Our IT solution provider(s) is not fully certified/competent to manage our compliance needs	15%	11%	12%	26%
Regulatory overload - Too many IT security and privacy regulations to comply with	10%	9%	10%	15%

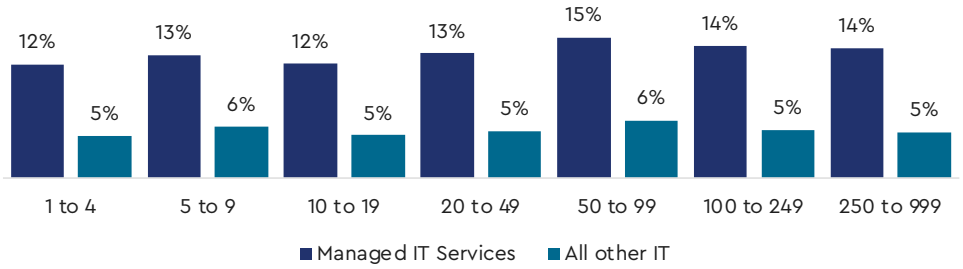
*Multiple answers allowed.

Figure 12. Staff entrusted with managing compliance (% of SMBs)*

	Total	North America	Europe	APAC
Senior/executive business leadership	46%	54%	35%	35%
Fully or partially managed by an external IT services company	29%	25%	20%	47%
Mid-level/line of business management staff/division heads	22%	18%	20%	32%
Risk, compliance or procurement specialist staff	18%	13%	13%	33%
No one in particular – we deal with it on a case-by-case basis	16%	17%	17%	12%
Finance/accounting staff	15%	14%	20%	15%
Fully or partially managed by an external legal services company	13%	7%	13%	27%
Internal legal staff	10%	10%	9%	10%

*Multiple answers allowed.

Figure 13. Annual IT spend growth (2021–2026 CAGR) over the next five years, by employees



Source: Analysys Mason SMB and TSP Research

Managed IT Services includes management of devices, networks, security , apps and cloud infrastructure/apps
All other IT includes hardware, software investments and spend on on-premise break-fix services

Appendix: Charts and Graphics

Figure 14. Self-reported share of annual IT budget spent on managed services, by geographic region (% of SMBs)

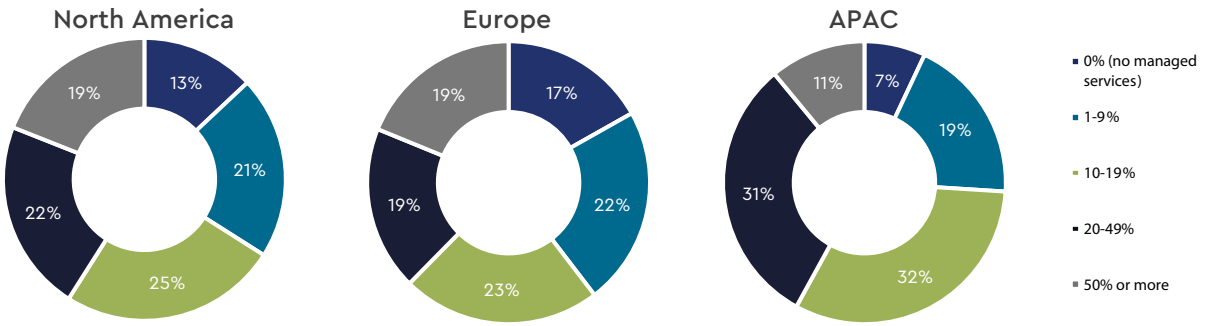
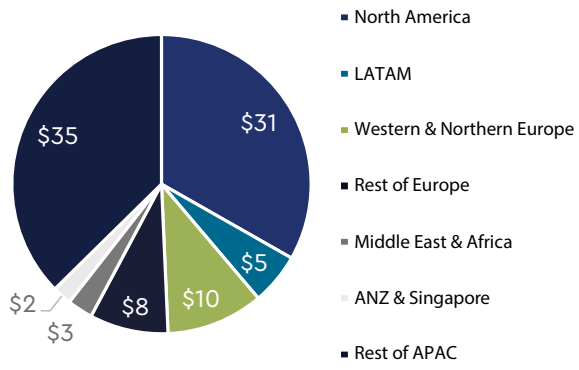


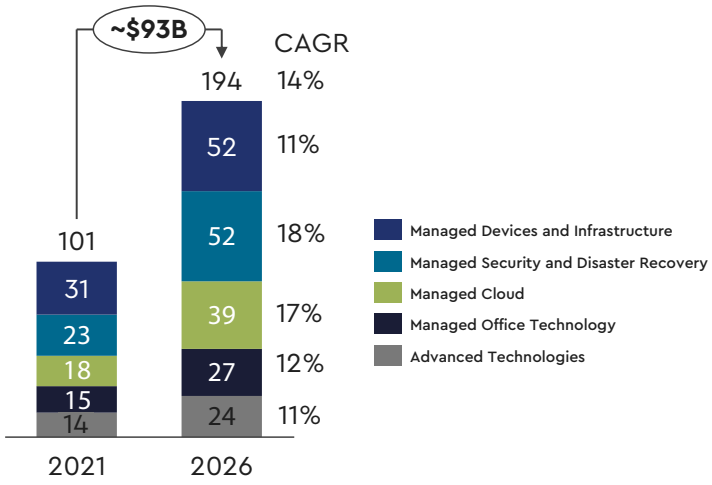
Figure 15. Regional net-new spending on managed IT services, 2021–2026



North America (US + Canada) will add over $30 billion in new spend between 2021-26, while other regions will add:

- Western & Northern Europe ~ $10 billion
- Rest of Europe ~ $8 billion
- ANZ and Singapore ~ $2 billion

Figure 16. Worldwide spending by businesses on managed IT services, 2021–2026



Appendix: Charts and Graphics

Figure 17. IT solution provider capabilities rated as "critical" by IT and business decision-makers*

*Multiple answers allowed.

Figure 18. Additional value on IT solution provider capabilities by businesses with over 50 employees (delta vs. smaller)*

*Multiple answers allowed.

Figure 19. MSPs' top 5 business challenges, by geographic region*

	North America	Europe	Asia-Pacific
1	Technician productivity improvement – 40%	Demand recovery after COVID – 31%	Time needed to launch new services – 38%
2	Getting clients to create budgets – 39%	Getting clients to create budgets – 26%	Getting clients to create budgets – 32%
3	Time needed to launch new services – 32%	Learning about new PSA, RMM tools – 26%	Technician productivity improvement – 27%
4	Learning about new PSA, RMM tools – 32%	Increasing competition – 24%	Increasing competition – 27%
5	Increasing competition – 31%	Technician productivity improvement – 23%	Learning about new PSA, RMM tools – 26%

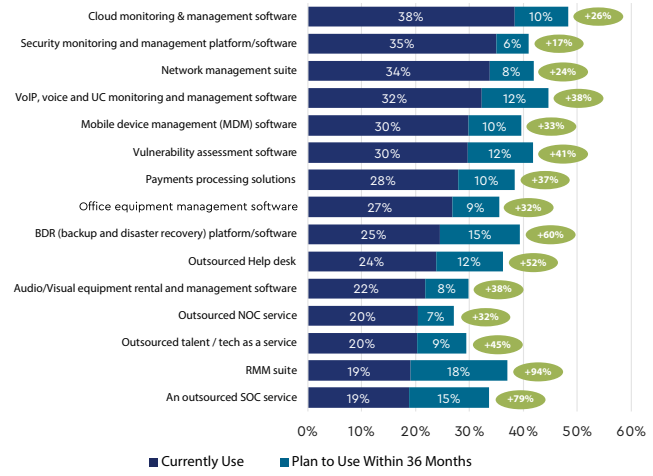
*Multiple answers allowed.

Appendix: Charts and Graphics

Figure 20. Managed IT services currently offered by MSPs and future portfolio expansion plans*

*Multiple answers allowed.

Figure 21. Monitoring management apps and platform usage and future adoption plans*



*Multiple answers allowed.

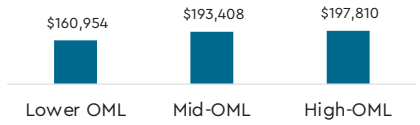
Figure 22. Key cybersecurity success factors cited by security-specialized MSPs*

*Multiple answers allowed.

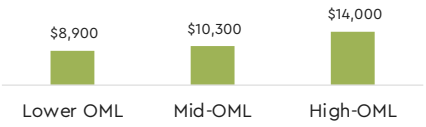
Figure 23. TSP average annual revenue per employee (top) and TSP average ARR per managed services (bottom)

Technology Solution Providers (TSPs) that follow best practices generate ~22% more revenue per employee, as well as ~50% higher average recurring revenue per account compared to peers that do not

TSP average annual revenue per employee



TSP average annual recurring revenue (ARR) per managed services account*



*Top accounts will generate significantly higher amounts, and a long tail will generate much lower amounts (80/20 rule); includes broader set of solution providers globally - MSPs, VARs, office technology and audio-visual providers; mix of account sizes are similar across all OML segments; data meant to illustrate OML-driven uplift – please do not use for pricing decisions

Source: Global TSP (MSP, VAR, AV and Office Technology Providers) survey underwritten by ConnectWise, N=1122

OML = Operational Maturity Level

High → Follow most best practices

Mid → Follow some best practices

Low → Follow few/none of the best practices