Acronis

Pulse of the Managed Service Provider 2021

Insights and Details

Table of Contents

Introduction, methodology, and demographics

As a follow-up to our [in-depth research project led](#) by Omdia (formerly Ovum) in 2020, Acronis conducted its own research among MSPs to take the pulse of the industry as it adjusts and adapts to the realities of a prolonged, global pandemic.

We conducted an online survey and received 244 responses from MSP managers and business leaders. Seventy-nine percent of the responses came from MSPs in North America, and the remaining 21% were spread out across the rest of the world.

Among the sample, 71% had been in business more than 10 years, 61% reported less than $2 million in annual revenue, and 73% had less than 100 customers. Other basic demographic information collected from respondents included age of business, annual revenue, client segmentation, and verticals served, as illustrated in the figures below.

Figure 1   **HOW LONG HAS YOUR COMPANY BEEN IN BUSINESS?**

0 to 5 years
11%
18% — 6 to 10 years
More then 10 years — 71%
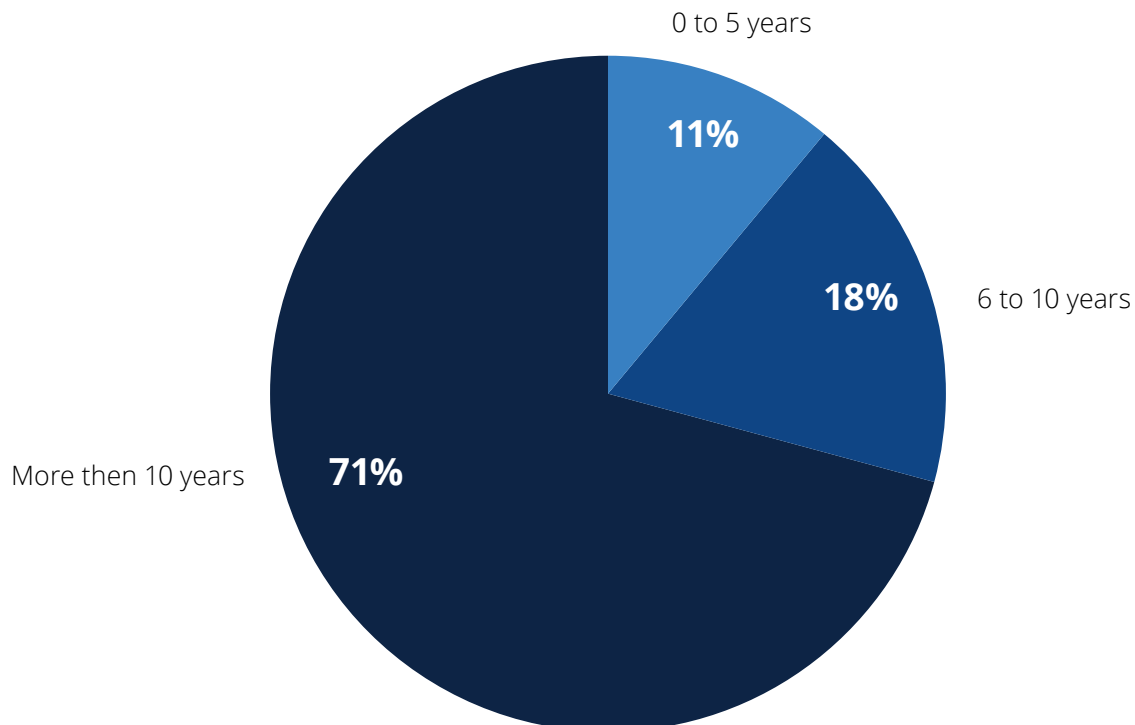
Figure 2   **WHAT IS YOUR ORGANIZATION'S TOTAL ANNUAL REVENUE? (USD)**

Don't know / prefer not to answer

$10 million or more

$5 million to $10 million

5%   **5%**   **5%**

41%   Up to $1 million

$2 million to $5 million   **23%**

20%

$1 million to $2 million
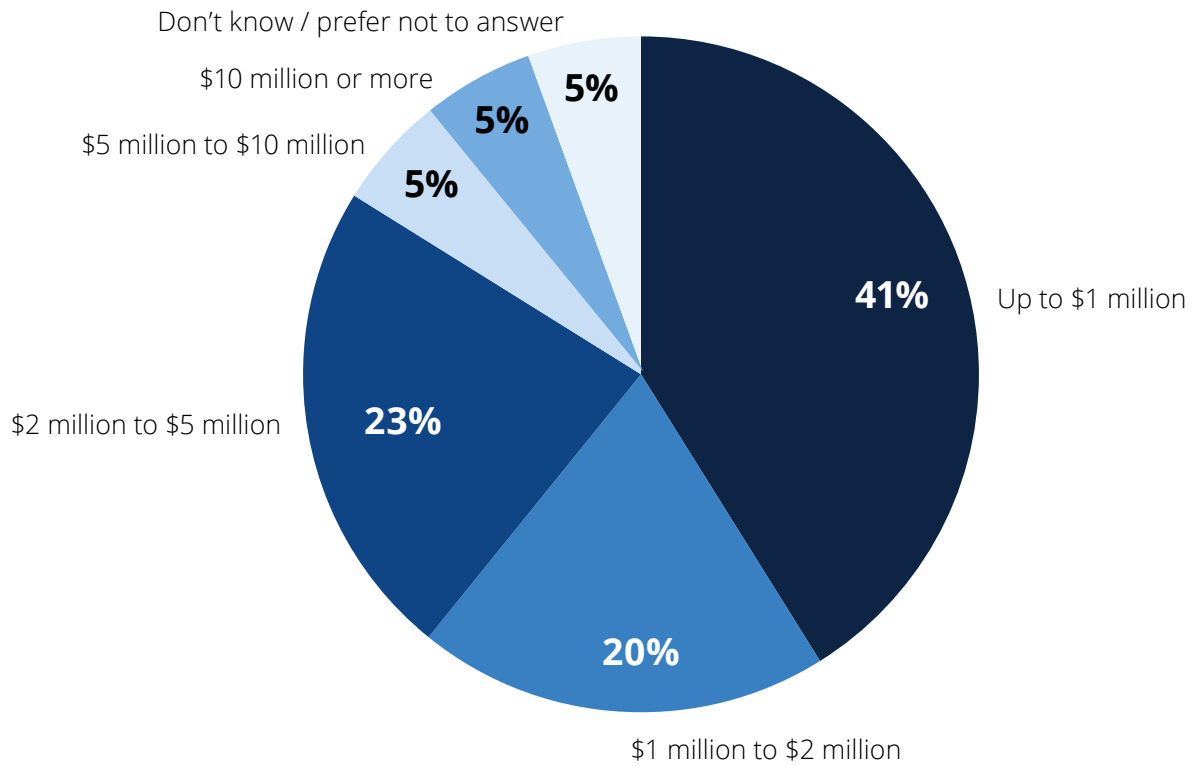
Figure 3   **CLIENT SEGMENTATION**

Enterprise (1000+ employees)

6%

Mid-market (100-999 employees)

13%

Public sector
(Government/Education)

4%

SMB (under 100 employees)   **77%**
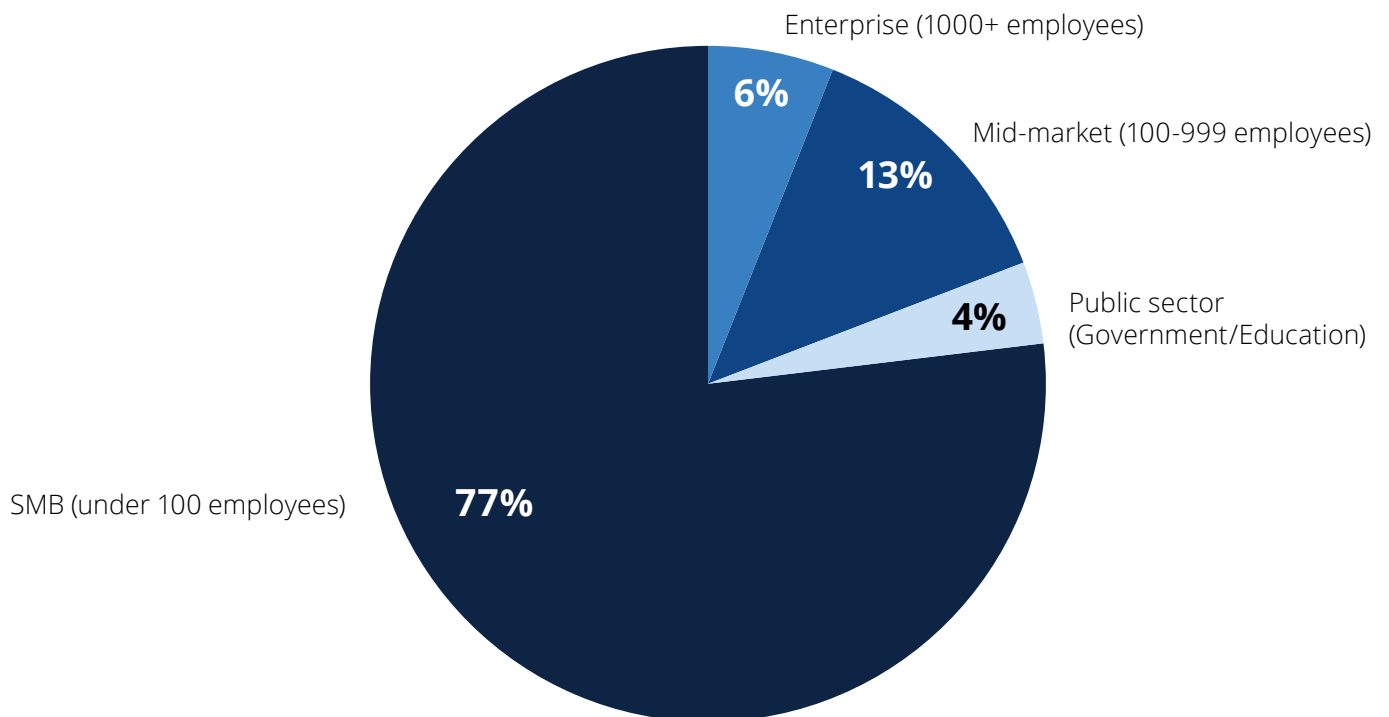
How demand changed in 2020

Given that businesses of all sizes had to react overnight to the restrictions and lockdowns resulting from COVID-19, we thought it was important to ask how demand for key managed services has changed since the beginning of 2020. Figure 4 paints a very clear picture that demand for supporting remote work and for managed security services is significantly increasing. We also see relatively strong demand for digital transformation services, and this also fits into the COVID-19 narrative, as end customers are having to reimagine their business processes and tools in order to adapt to the new market realities.

Figure 4

HOW WOULD YOU CHARACTERIZE CLIENT DEMAND FOR THE FOLLOWING SERVICES SINCE THE START OF 2020?

Legend: Significantly Decreasing · Moderately Decreasing · Staying Same · Moderately Increasing · Significantly Increasing

Categories: For remote Work support · For Cybersecuruty · For Digital Transformation · For Cloud Migrations · For Governance · For Unified Communications · For Network… · For Systems Integration Projects · For Help Desc · For Data Center Shutdowns
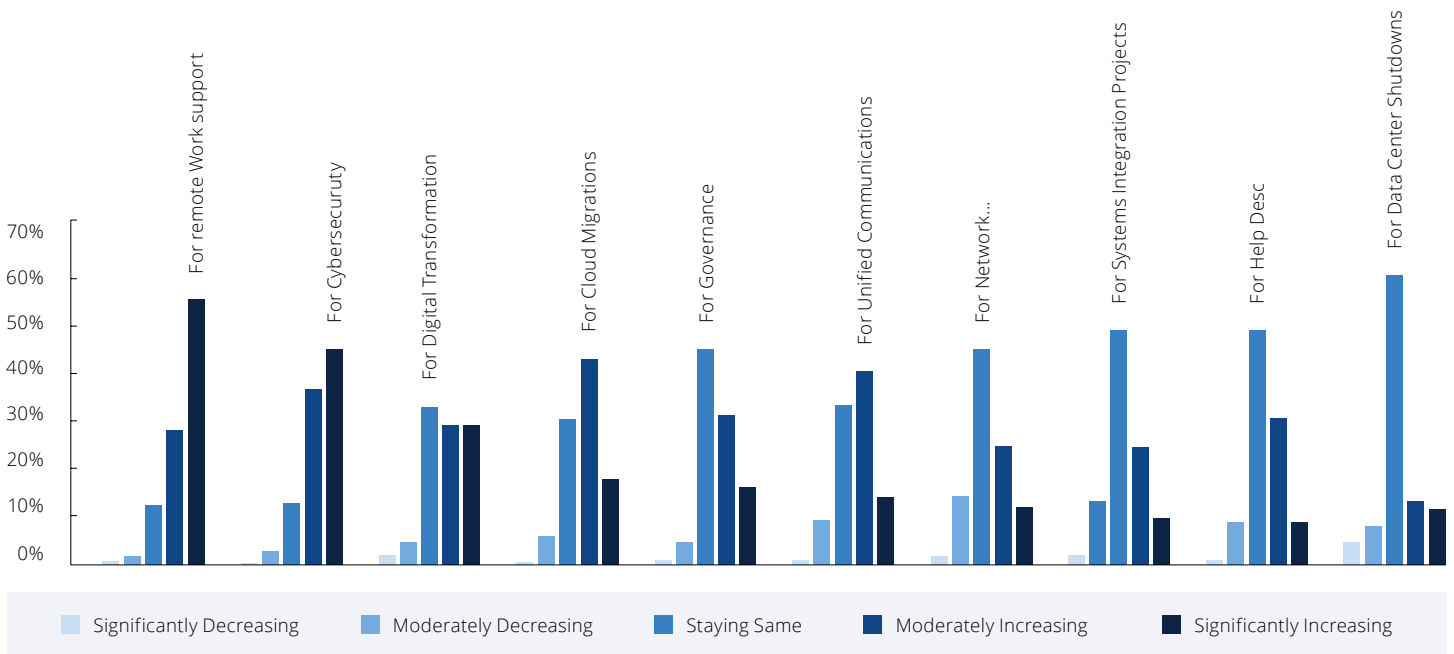
Trends in demand for services are having a clear and significant impact on how MSPs expect their businesses to change over the next two years. As shown in Figure 5, MSPs anticipate their top generating services to be heavily focused on offering managed security and cloud-based managed solutions. All other historically meaningful areas of MSP business will be contracting — with the exception of software resale, which will remain unchanged. In short, what it means to be an MSP is fundamentally changing, and quickly. While it is safe to say that these changes were already underway, the realities of COVID-19 have amplified and accelerated the industry's evolution.

Figure 5   **HOW WILL THE TOP REVENUE GENERATING SERVICES THAT YOU PROVIDE CHANGE OVER THE NEXT TWO YEARS?**
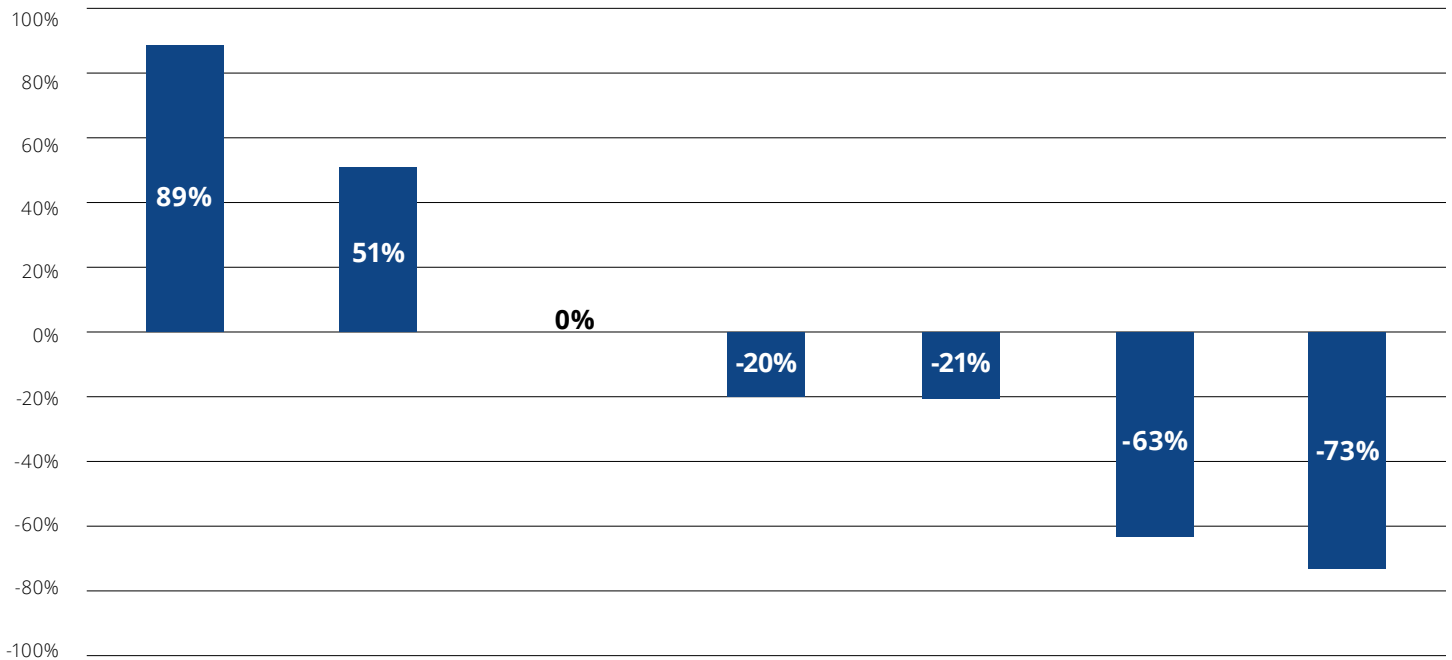
■ Change over next two years

|	
89%	Manage security services
51%	Cloud-based managed services (e.g. SaaS, IaaS)
0%	Value-added professional services
-20%	Software resale
-21%	Remote managed and network services
-63%	Hardware resale
-73%	Traditional support services

Why this matters and how Acronis can help

Your business is fundamentally changing, and this was no doubt accelerated by COVID-19. If you are still conducting "business as usual" with a product portfolio and strategy from ten years ago, the data suggests your business will be struggling within the next couple of years. If you haven't done so already, it is time to start transforming. The future is in offering cloud-based solutions and managed security.

Acronis enables service providers to deliver cyber protection in an easy, efficient, and secure way. With one solution, MSPs and their clients gain access to cloud-based solutions such as backup, disaster recovery, file sync and share, and blockchain-based file notarization — as well as managed security services including AI-based anti-ransomware and anti-cryptojacking, and vulnerability assessment capabilities with patch management, all managed from a single console.

Figure 6   DELIVERING CYBER PROTECTION WITH ACRONIS
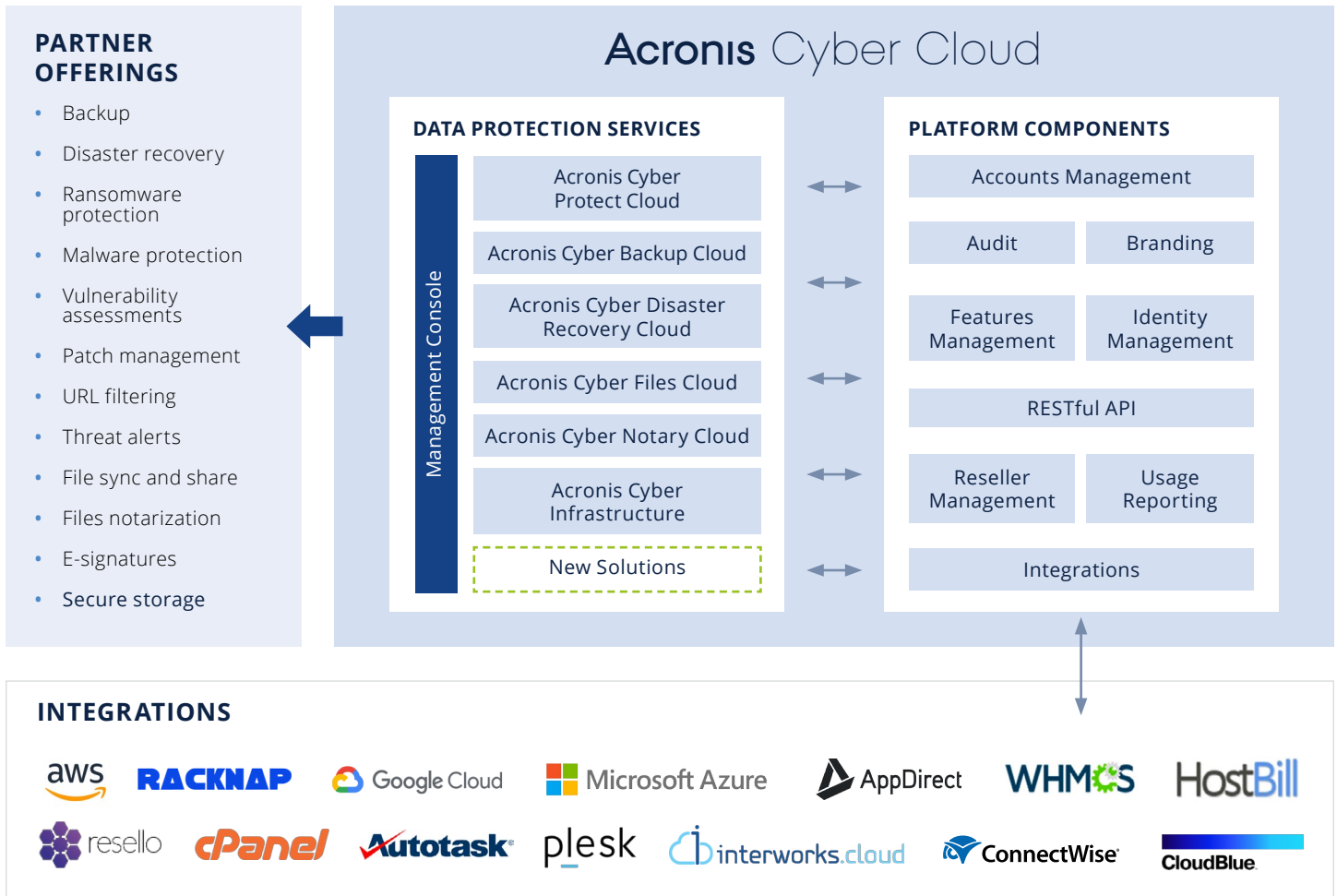
Offering security services and working with security vendors

MSPs clearly view offering managed security as central to their business in the immediately future. As such, the remaining questions covered in this report drill deeper into the operational realities of offering managed security services.

First, we asked about the top five revenue-generating security services currently offered, and how this is expected to change in the next two years. There was one notable shift found in the data which aligned to the broader changes in being an MSP outlined in Figure 5 above. Namely, remote monitoring and management (RMM) fell out of the top five and it was replaced by cloud/SaaS security and backup, which took the overall top spot. Also of note was that governance, risk, and compliance support was tied for fifth in two years. We see this as an offshoot of the broader evolution towards managed security.

Figure 7 — WHAT ARE THE TOP FIVE REVENUE-GENERATING SECURITY SERVICES YOU PROVIDE TODAY, AND HOW WILL THIS CHANGE IN TWO YEARS?

TODAY

1. **Network security** (e.g., DNS filtering, managed gateways, managed firewall)
2. **Endpoint protection** (antivirus, anti-malware)
3. **Data protection** (backup/ recovery/disaster recovery)
4. **Remote monitoring and management** (RMM)
5. **Email security** (encryption, spam filtering)

IN TWO YEARS

1. **Cloud/SaaS security and backup**
2. **Network security** (e.g., DNS filtering, managed gateways, managed firewall)
3. **Data protection** (backup/recovery/ disaster recovery)
4. **Endpoint protection** (antivirus, anti-malware)
5. **TIED**:

   a. **Email security** (encryption, spam filtering)

   b. **Governance, risk, and compliance support**

OTHER SECURITY SERVICES LISTED

- Identity and access management
- Vulnerability scanning / assessment
- Remote managed and network services
- Security awareness training/ education
- Remote monitoring and management (RMM)
- Patch management
- Dark web monitoring
- Security audit and forensic support
- Outsourced security operations centers
- Data loss prevention (DLP)
- Intrusion detection / management
- VPN
- Web content / URL filtering
- Web server security analysis / monitoring / protection
- Penetration testing
- Anti-phishing operations

To gain some additional insight into the revenue being generated from these services, we asked MSPs what their biggest challenges were in selling managed security services. The biggest challenge reported overall was **educating potential clients on the need** — particularly the need to pay more for these services. This makes a lot of sense, considering that SMBs' budgets are tight and the MSP is asking them to spend money on prevention rather than on fixing their current challenges. **Vendor selection** and **integration of security offerings** were the next two most popular, and we drill into these answers below.

Figure 8   **WHAT ARE THE BIGGEST CHALLENGES IN SELLING MANAGED SECURITY SERVICES?**

1 Educating potential clients on the need

2 Vendor selection

3 Integration of security offerings with existing business and IT systems (e.g., provisioning, billing)

Longer, more complex sales processes and cycle
Recruiting and retaining security experts
Re-training sales teams to sell security
Adjusting business model and compensation plans to reflect an annuity model
Customer billing logistics (including metering, integration)
Recruiting qualified sales people
Providing self-service ordering for customers
Competition

Considering that vendor selection was of significant importance, it is interesting to see how many security vendors MSPs are working with. Seventy percent reported between two and five. The second most common response was zero, meaning these MSPs either don't currently offer managed security services or they do so completely in-house.

Figure 9   **HOW MANY SECURITY VENDORS DO YOU WORK WITH?**

- **4%** Don't know prefer not to say
- **4%** None
- **5%** 1
- More than 5 **18%**
- **70%** 2 to 5
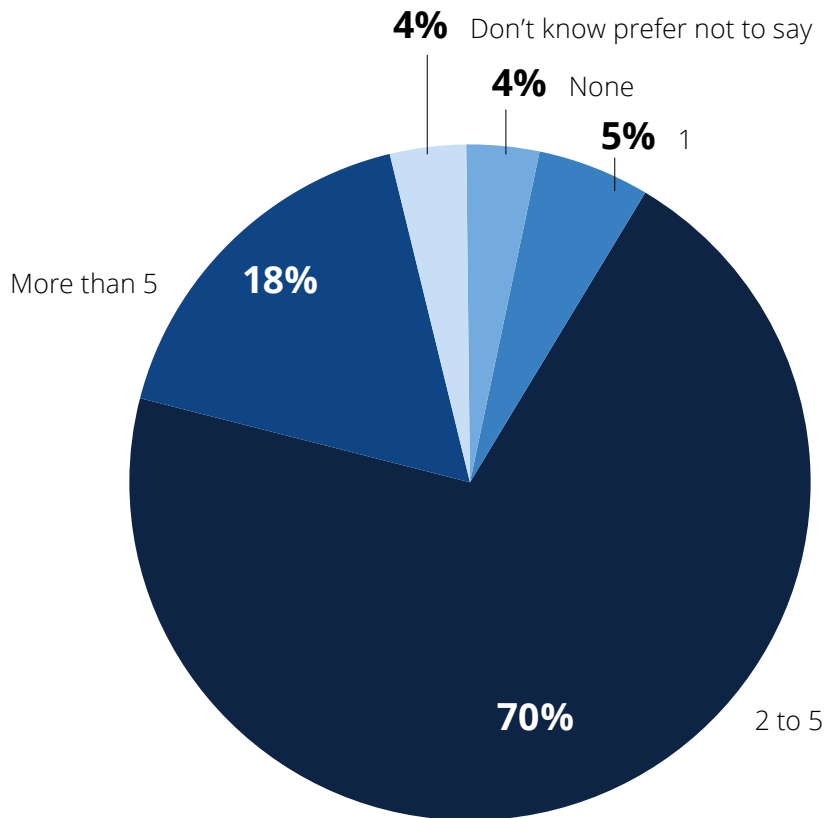
Figure 10 PLEASE RANK THE FOLLOWING IN ORDER OF IMPORTANCE WHEN IT COMES TO SELECTING A PREFERRED VENDOR?

1 Vendor product features

2 Quality technical support and training

3 Integration with my PSA and RMM systems

4 White label options

5 Margin/incentives

Interestingly, **integration with PSA/RMM systems** was in the middle, although it was one of the top challenges the same MSPs reported when it came to selling managed security services. To learn more, we asked which of the security services offered (found in Figure 8) they would prefer to be integrated into a single platform.

This could include technical integration, such as having a common administrative console/portal, or operational integration, such as billing and support ticketing. MSPs could only choose five services they preferred to be integrated. Figure 12 shows the top selections.

Figure 11 WHICH OF THESE SERVICES WOULD YOU PREFER TO BE INTEGRATED INTO A SINGLE PLATFORM?

1 Endpoint protection (antivirus, anti-malware)

2 Network security (e.g., DNS filtering, managed gateways, managed firewall)

3 Vulnerability scanning / assessment

4 Intrusion detection / management

5 Data protection (backup/recovery/disaster recovery)

One of the consequences of having unintegrated services is having numerous agents per endpoint. This can lead to operational inefficiencies for updates as well as security and downtime risks. Quite simply, multiplying each agent by the number of endpoints being managed equates to the number of potential issues that exist in an MSP's footprint.

Running more agents makes the deployment of every machine more complicated and creates potential incompatibility problems, as well as degrading performance. Figure 13 asks MSPs how many agents they are running. While 51% report between only one to three agents, 22.5% report having seven or more agents in production.

Figure 12 **WHAT IS THE AVERAGE NUMBER OF AGENTS RUNNING ON A GIVEN ENDPOINT THAT YOU MANAGE?**

0 / Don't know / Don't manage endpoints

7.6%

10+ 14.5%

7 to 10 8.0%

51.0% 1 to 3

4 to 6 19.7%
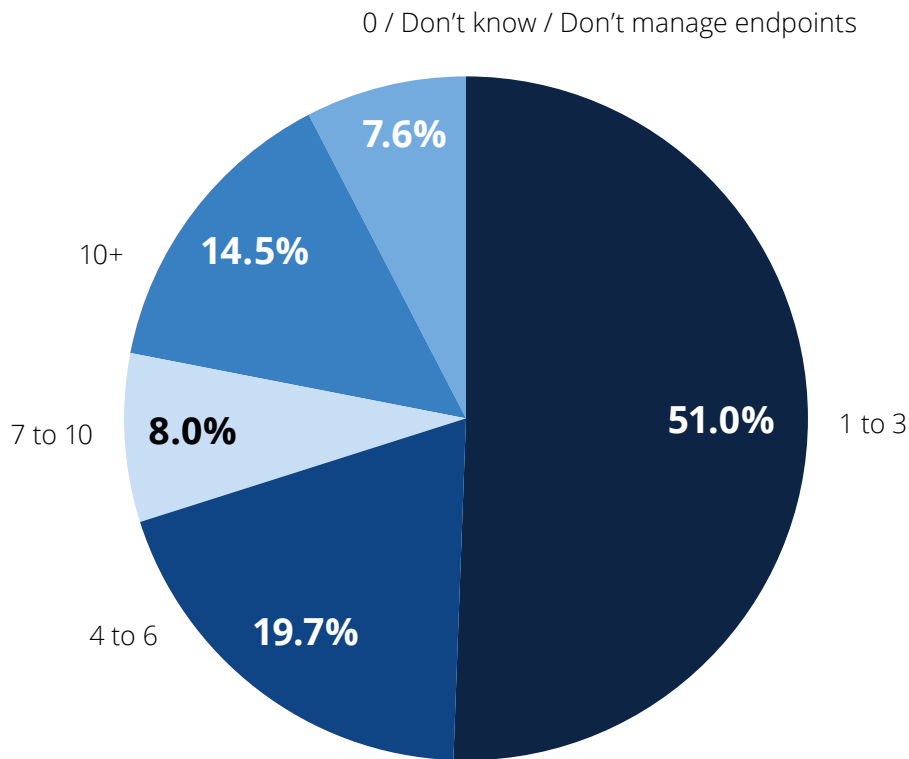
Why this matters and how Acronis can help

Having explored the operational realities of offering managed security services, there are three main takeaways that make Acronis particularly relevant to the research results:

The importance of offering the right, integrated services

Looking at the tables in Figures 6 and 10, most of the top revenue-generating services today and in two years are available from Acronis. Not only does Acronis enable MSPs to sell many of the most essential managed security services, but it does so through a single administrative console. Furthermore, technical integration allows for many unique product features. For example, backups receive antivirus scans during restoration in order to prevent any infected files from being put into production.

Integrate third party tools with the Acronis Cyber Platform

In addition to the Acronis products being integrated with each other, Acronis offers an open API, SDKs, and developer support, enabling easy integration with RMM, PSA, cloud targets, or any proprietary applications. This allows MSPs to automate virtually any aspect of their operations.

Minimize agents running on endpoints

With Acronis, you only need one agent as opposed to needing 6+ agents to offer backup, disaster recovery, AI-based anti-ransomware and anti-cryptojacking, vulnerability assessments and patch management, file sync and share, and e-signature services. This creates operational efficiencies while reducing risk, and it improves the performance of clients' machines.

For more information

Learn how you can transformyour MSP business with Acronis:

Discover more information in the Acronis Resource Center   READ ON

Get a complimentary 30-day trial of Acronis Cyber Protect Cloud   TRY NOW

Reach out to Acronis directly   REQUEST DEMO

Learn more at
www.acronis.com