

REPORT

MSP PERSPECTIVES 2026

Insights from 800 MSPs into the challenges and opportunities shaping the future of cybersecurity services.

SEPTEMBER 2026



Executive summary

Cybersecurity is facing a leadership crisis. There is just one Chief Information Security Officer (CISO) for every 10,000 organizations globally¹, leaving the vast majority without the dedicated stewardship and strategy they need to be verifiably secure. Meanwhile, to compound the issue, incidents keep rising, security spend is up, and boardroom confidence remains low. Organizations may be investing more than ever, but many still struggle to answer fundamental questions about their risk, resilience, and investment outcomes.

This gap presents a major opportunity for Managed Service Providers (MSPs) and other channel experts to step beyond delivery and become trusted cyber leaders. The research in this report shows that customers are increasingly looking to their partners for guidance across their cyber program, from technical implementation through to full management. The partners that can bring clarity to complexity, helping their customers see where they stand, how they are improving, and where risk remains, will be best positioned to fill this leadership void.

However, delivering cybersecurity leadership at scale requires more than expertise alone. As shown on page 19, **MSPs estimate they could save more than half of their team's time** if security and compliance activities were managed through a single, unified platform. This highlights the crucial importance of operational efficiency. To meet growing customer demand, providers need a model that makes their efforts repeatable, scalable, and measurable across their customer base.



Scott Barlow
VP, Chief Evangelist
Sophos

¹ <https://www.sophos.com/en-us/resources/report/2026-ciso-report>

Introduction

The Sophos MSP Perspectives 2026 report provides insights into three strategic areas of MSP business:

- The rise of MSP-delivered cyber leadership
- Compliance as the core of MSP service delivery
- Operationalizing security and compliance at scale

Findings are based on an independent, vendor-agnostic survey of 800 MSPs located across the U.S. (200), U.K. (100), Germany (100), France (100), Singapore (100), Australia (100), and Brazil (100). Respondents represent senior to board-level MSP stakeholders.

The survey was commissioned by Sophos and conducted by research house Vanson Bourne in April 2026.

800

MSPs

7

Compliance areas in focus

7

Countries

Key findings at a glance

1. MSPs have become the de facto CISOs for their customers

- **88%** of MSPs say at least **20%** of their customers look to them to act as their CISO.
- **84%** of MSPs expect demand for CISO services to increase over the next 12 months.

2. Compliance services are widespread, but not mature

- **99%** of MSPs provide compliance services.
- **6%** provide a comprehensive compliance service stack, leaving room for growth.

3. Compliance drives security investment

- **50%** of customer purchasing decisions are influenced by compliance demands.
- This influence is a major factor in **33%** of purchasing decisions on average.

4. The shift to continuous compliance is gradual

- **62%** of MSPs are "very confident" in their ability to continuously monitor, manage, and document compliance across multiple customers.
- **33%** are "completely confident", highlighting that many would benefit from improvement.

5. Tool-based delivery is the standard

- **53%** of MSPs use multiple tools or platforms to centrally manage cybersecurity compliance or CISO-type activities.
- **36%** rely on just one, implying that MSPs and their customers operate within a model that is complex, fragmented, and potentially incomplete.

6. Security reporting is becoming automated

- **86%** of MSPs use a fully- or semi-automated process for producing consolidated security posture reports.
- **55%** still require manual effort to consolidate activities, suggesting most reporting processes remain only partially automated.

7. Significant efficiency gains remain untapped

- **53%** is the time MSPs would save if they could use a single, unified platform for customer security posture and compliance management and reporting.
- **81%** of MSPs believe it would reduce the time they currently spend on these activities by more than **30%**.

Part 1: The rise of MSP-delivered security leadership

1. MSPs have become the de facto CISO for their customers

Organizations face growing pressure from an evolving threat landscape, artificial intelligence (AI)-powered attacks, expanding regulations, and the security skills shortage. Many also lack the in-house leadership needed to address these challenges through a coordinated cybersecurity program rather than technology management alone. In response, MSPs are moving up the value chain, evolving from tactical tooling providers to strategic advisory partners.

The report data shows this shift is well underway. On average, MSPs estimate that **46% of their customers** now rely on them for this type of cyber leadership. This reliance is widespread: **88% of MSPs** act as the CISO for more than **20%** of their customer base, **40%** for more than half, and **20%** for more than **70%**.

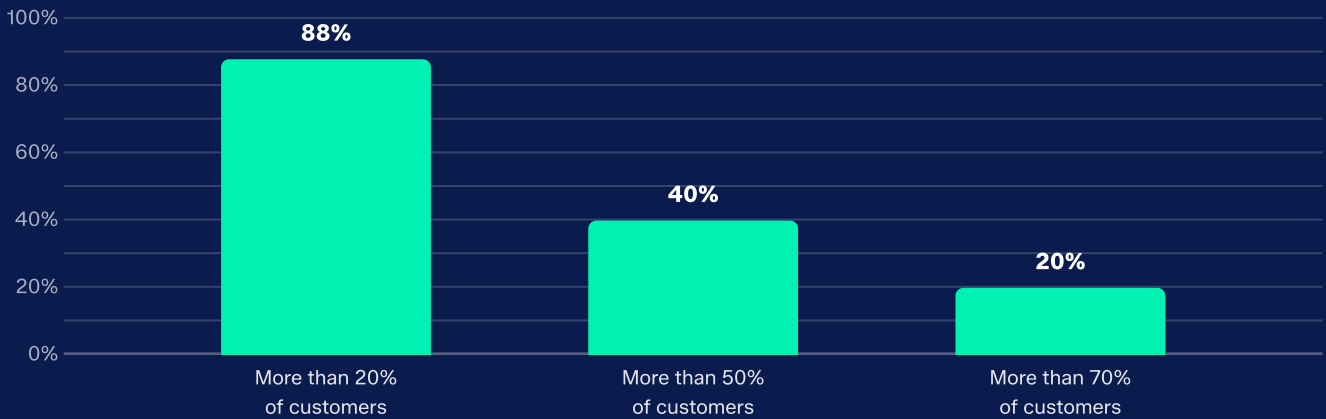
88%

of MSPs are acting as the CISO for more than 20% of their customer base.

46%

of MSP customers, on average, look to their MSP to act in this capacity.

Customer reliance on MSP-delivered CISO services

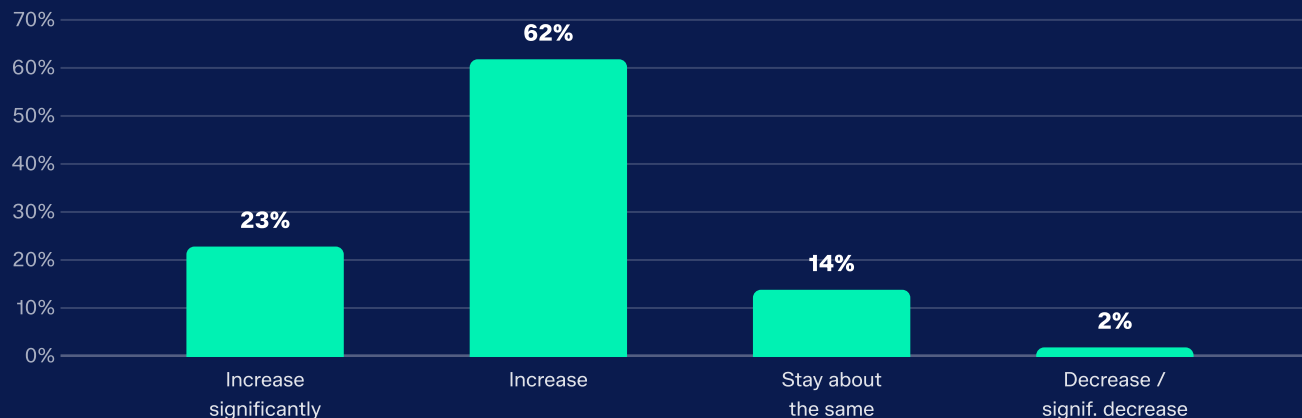


Approximately what percentage of your customers look to your organization to act as their CISO, if any? (n=800)

Demand for MSP-delivered CISO services will increase

This opportunity for MSPs is only set to grow. **84%** expect demand for CISO services to increase over the next 12 months, including **23%** who anticipate significant growth. Only **2%** expect a decrease.

Expected change in demand for CISO services



How do you anticipate this will change in the next 12 months, if at all? (n=800)

The traditional boundaries of the MSP role are rapidly changing, reflecting the challenges faced by organizations that lack the expertise, resources, or funds to support a dedicated, in-house security leader. They now look to their MSPs for CISO-level strategic cybersecurity guidance, risk management, and governance that extends beyond day-to-day technology management. The providers who can step into this gap and establish themselves as the go-to are well positioned to take on increasing demand.

84%

of MSPs expect demand for CISO services to increase over the next 12 months.

23%

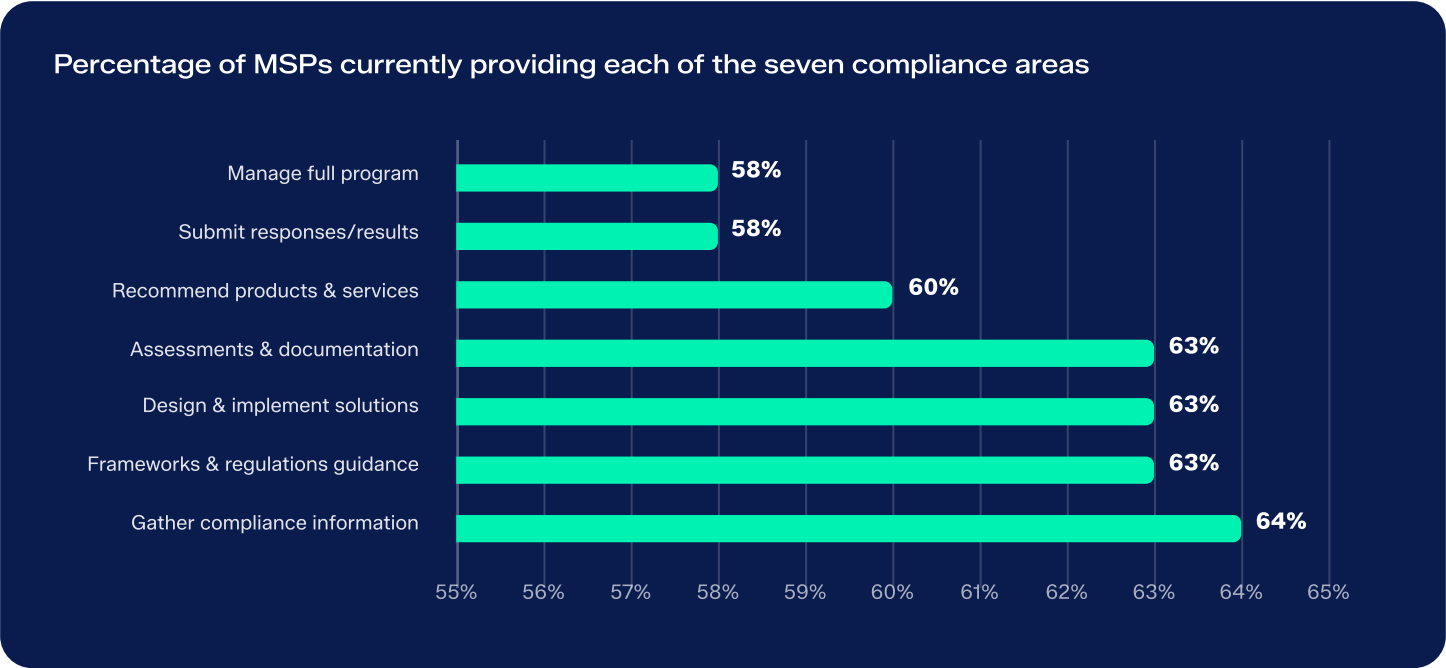
expect it to increase significantly.

Part 2: Compliance as the core of MSP service delivery

1. Compliance services are widespread, but not mature

Cybersecurity compliance is now a mainstream part of the MSP value proposition, driven by increasing regulations and laws that require dedicated, continuous cyber program management. MSPs are incredibly well suited to deliver this.

Across the seven compliance activities measured, service provision is consistently strong. For each service area listed, **58% to 64% of MSPs** say they already provide that specific capability to customers.



Which of the following best describes your organization's involvement in customers' cybersecurity compliance today, and in the future? (n=800)

99%

of MSPs provide some level of compliance service.

58%

provide full program management.

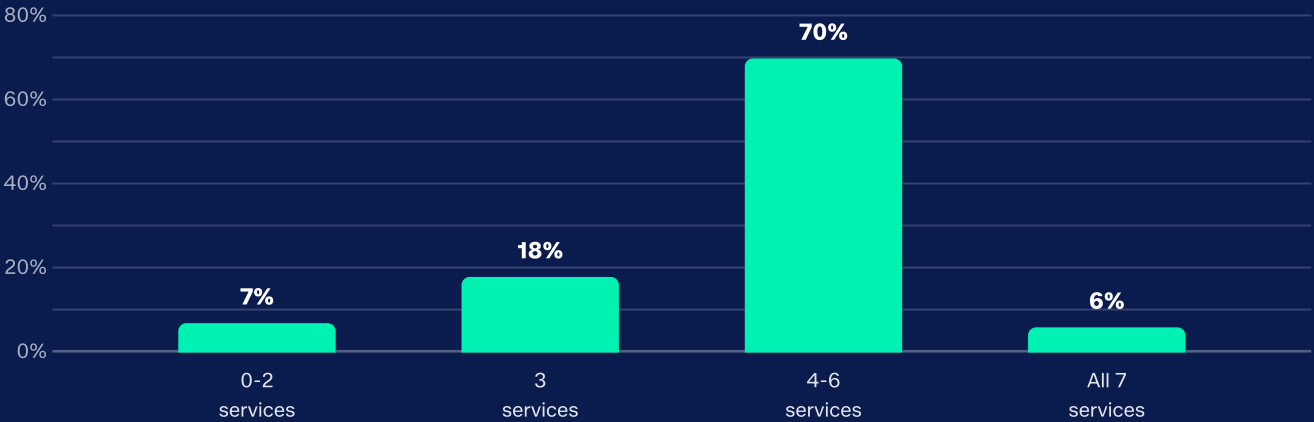
6%

provide a comprehensive compliance service stack.

Few MSPs offer the full suite of compliance services

While individual compliance services are widely offered, most MSPs stop short of delivering the complete compliance lifecycle; **70%** offer between four and six of the seven activities measured, while just **6%** provide all seven. This suggests that many MSPs still need to expand their offering and connect these capabilities into an end-to-end compliance program that delivers the comprehensive oversight customers need.

Depth of compliance services offered

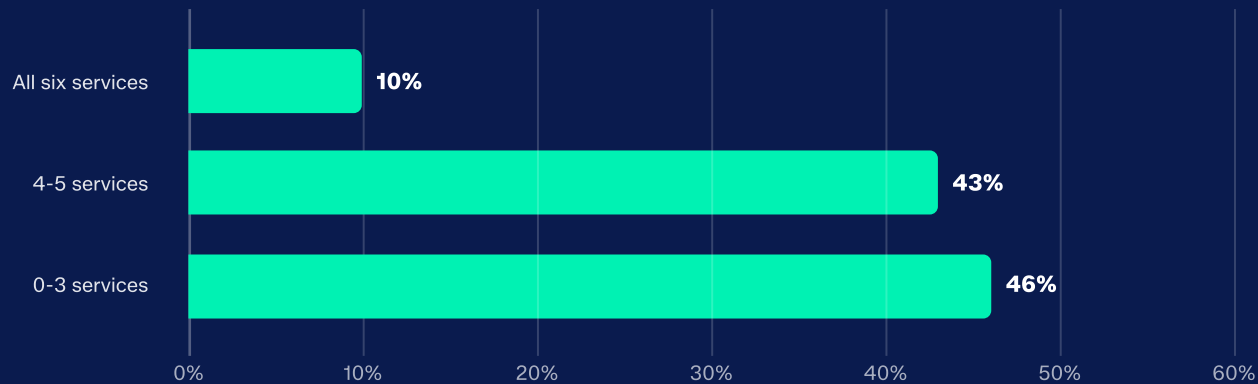


Which of the following best describes your organization's involvement in customers' cybersecurity compliance today, and in the future? (n=800)

Many MSPs providing compliance program management don't offer all supporting services

Looking specifically at MSPs that manage their customers' full compliance program reveals a similar gap. Of the **58% of MSPs** who do so, only **10%** also provide the other six services. This suggests many MSPs are taking on program-level responsibility before building a comprehensive compliance service stack. In practice, compliance program management may involve coordinating activities performed by customers or third-party specialists, rather than delivering each service directly. As a result, program oversight and service delivery capability do not always go hand-in-hand.

Number of compliance services delivered by MSPs offering full program management



Which of the following best describes your organization's involvement in customers' cybersecurity compliance today, and in the future? MSPs providing full compliance program management (n=465)

MSPs plan to grow their compliance offering

The good news is that demand for these capabilities is likely to drive further expansion. Many MSPs that do not currently deliver compliance services plan to introduce them in the future. The strongest growth is expected in full compliance program management: beyond the 58% already delivering this capability, a further 40% plan to add it. This suggests program management is rapidly becoming a standard component of MSP compliance offerings.

SERVICE	CURRENTLY OFFERING	PLAN TO INTRODUCE	TOTAL
Recommend products/services Advise on security tools and services that support compliance objectives.	60%	38%	99%
Design & implement solutions Configure and deploy security controls to meet compliance requirements effectively.	63%	37%	100%
Frameworks & regulations Identify applicable regulations, standards, and frameworks affecting customer compliance.	63%	36%	99%
Gather compliance information Provide the evidence customers need to satisfy compliance obligations.	64%	35%	99%
Assessments & documentation Perform assessments and create documentation demonstrating compliance status and gaps.	63%	36%	98%
Submit responses/results Prepare and submit audit responses, questionnaires, and compliance evidence.	58%	40%	98%
Manage full program Oversee ongoing compliance activities, evidence collection, reporting, and governance.	58%	40%	99%

Percentages are rounded.

Which of the following best describes your organization's involvement in customers' cybersecurity compliance today, and in the future? Excludes "Don't know" (n=800)

Compliance services are a growth area for MSPs of all sizes

The maturity of MSPs' compliance offering is not defined by their size. While MSPs with 51+ employees are most likely to provide all seven measured compliance services **(10%)**, smaller MSPs are still competitive. Those with up to five employees are more likely to provide four to six of the seven services **(77%)** than any other group and report the highest average number of services delivered.

Adoption of full program management is also relatively consistent, ranging from **54% to 62%**. This suggests compliance is becoming a growth area for MSPs of all sizes, shifting competition from service availability towards delivery speed, depth, and maturity.

MSP SIZE	0-2 SERVICES	3 SERVICES	4-6 SERVICES	ALL SEVEN SERVICES	AVERAGE # OF SERVICES	FULL PROGRAM MANAGEMENT
1-5 employees	5%	11%	77%	7%	5	62%
6-25 employees	8%	25%	65%	2%	4	54%
26-50 employees	8%	17%	70%	6%	4	59%
51+ employees	5%	17%	69%	10%	4	59%

Percentages are rounded.

Which of the following best describes your organization's involvement in customers' cybersecurity compliance today, and in the future? Excludes "Don't know" (n=800)

MSPs have made significant progress building compliance practices, with almost all providers now offering at least one compliance service and the majority delivering multiple capabilities across the compliance lifecycle. Full program management is becoming mainstream and is on track to become an almost universal offering, reflecting growing customer demand for ongoing compliance support.

Service breadth should not be mistaken for maturity, however. While many MSPs have expanded beyond basic advisory services, relatively few have developed a truly complete compliance offering. Most continue to operate with partial service stacks. Even among those delivering full program management, only a small minority provide the complete set of supporting compliance services.

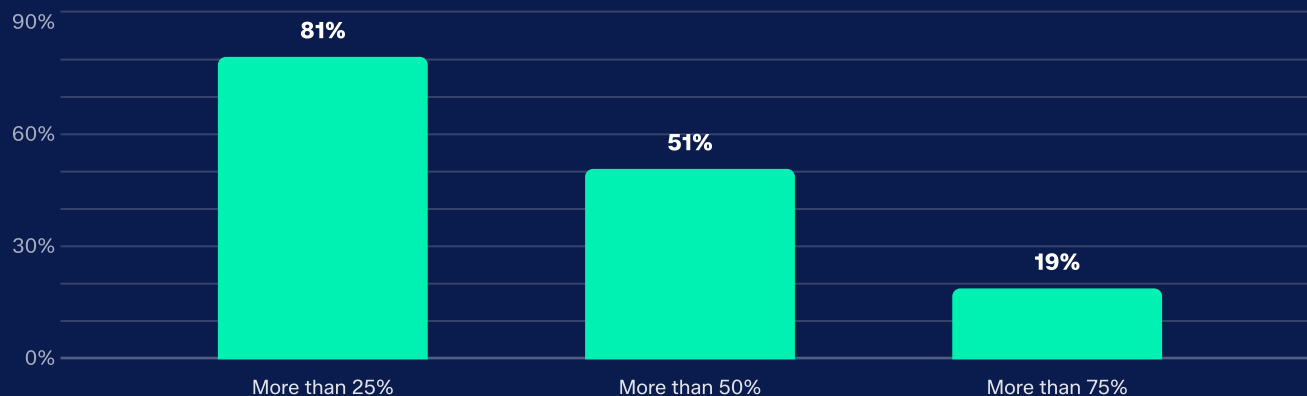
As compliance services become more widely available, competitive advantage will increasingly depend on the speed, depth, quality, and seamlessness of delivery rather than provision alone. **MSPs that can connect advisory, implementation, documentation, reporting, and program management into a cohesive compliance practice will be best positioned to differentiate themselves as the market leaders.**

2. Compliance drives security investment

Compliance is now a meaningful driver of cybersecurity investment. MSPs say that compliance influences **50%** of customer cybersecurity purchases on average, with **33%** of decisions shaped “heavily” or “decisively”. That influence is widespread: **81% of MSPs** say compliance affects at least **25%** of customer purchases, and **51%** say it influences at least half. In other words, compliance is no longer just a reporting requirement and is actively shaping how customers prioritize security spend.

The opportunity is now to make that influence more strategic. Only **9%** of MSPs say compliance “heavily” or “decisively” influences a significant majority (**75%**) of customer cybersecurity purchases. This leaves headroom for MSPs to use compliance as a gateway into broader advisory conversations, deeper services, and more structured security programs.

Percentage of customer purchases influenced by compliance



What percentage of your customers' cybersecurity purchasing decisions are influenced, at least in part, by regulatory compliance requirements, if any? (n=800)

50%

of customer purchasing decisions are influenced by compliance demands.

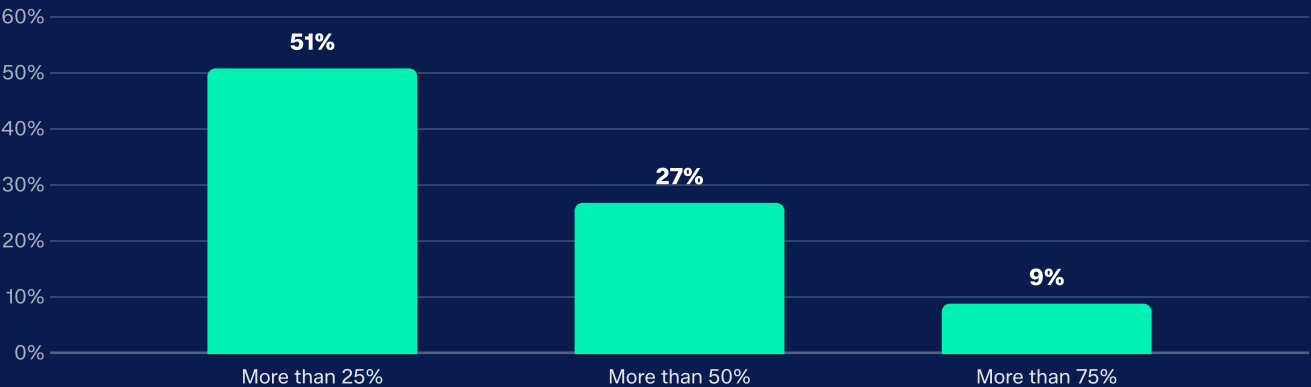
33%

of those decisions are heavily influenced by regulatory compliance demands.

MSPs can use customer compliance to inform strategic conversations

Taken together, the findings show that compliance is moving from a regulatory obligation to a key business driver. It already has a clear influence on customer security spend. However, few MSPs have made it a lucrative route into broader cybersecurity conversations. This provides space for them to fill the gap and turn compliance-led demand into deeper advisory relationships and higher-value strategic services.

Percentage of customer purchases "heavily" or "decisively" influenced by compliance

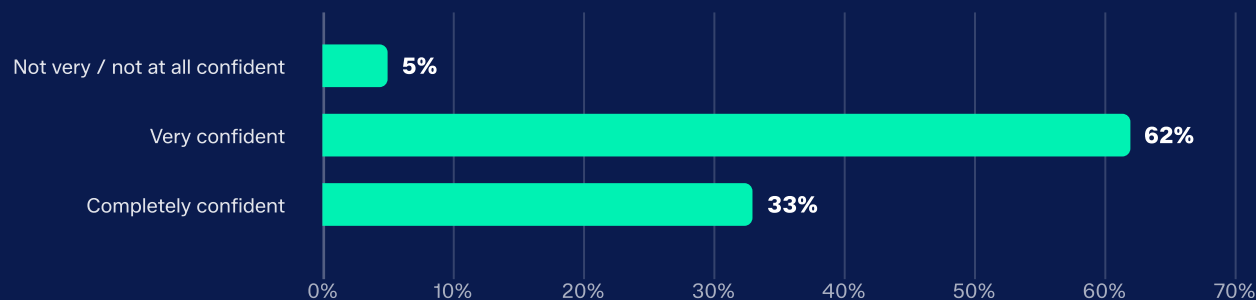


What percentage of your customers' cybersecurity purchasing decisions are heavily or decisively influenced by regulatory compliance requirements? (n=800)

3. The shift to continuous compliance is gradual

MSPs are increasingly adopting a continuous approach to compliance management. Confidence levels suggest most providers believe they are well equipped to support customers as compliance moves from periodic audits to ongoing monitoring and governance. Overall, **95% of MSPs** are either “very” or “completely” confident in their ability to continuously monitor, manage, and document compliance across multiple customers.

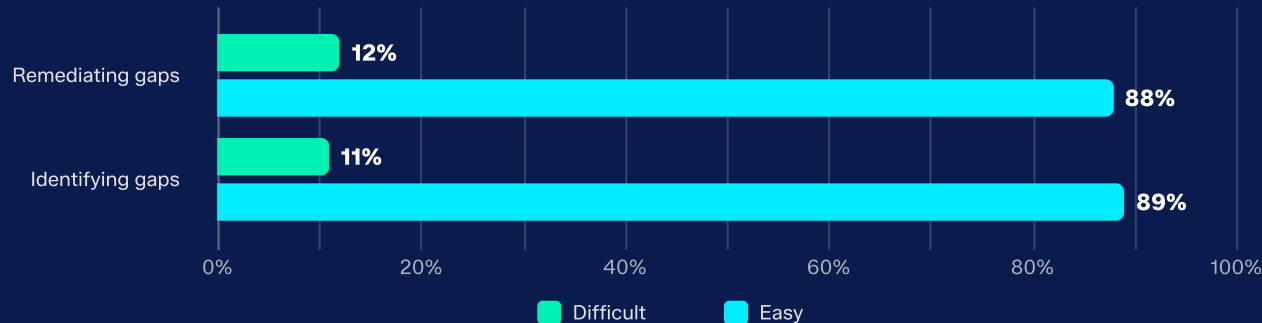
MSP confidence in managing continuous compliance



How confident are you in your organization's current ability to continuously monitor, manage, and document compliance requirements across multiple customers, if at all? (n=800)

This confidence is also reflected in how equipped MSPs are to identify and remediate compliance and control gaps for their customers, with only a small minority reporting difficulties with both.

MSP ease at finding and remediating compliance and control gaps



How easy or difficult is it for your organization to identify and remediate compliance or control gaps for your customers today? (n=800)

62%

of MSPs are “very confident” in their ability to continuously monitor, manage, and document compliance across multiple customers.

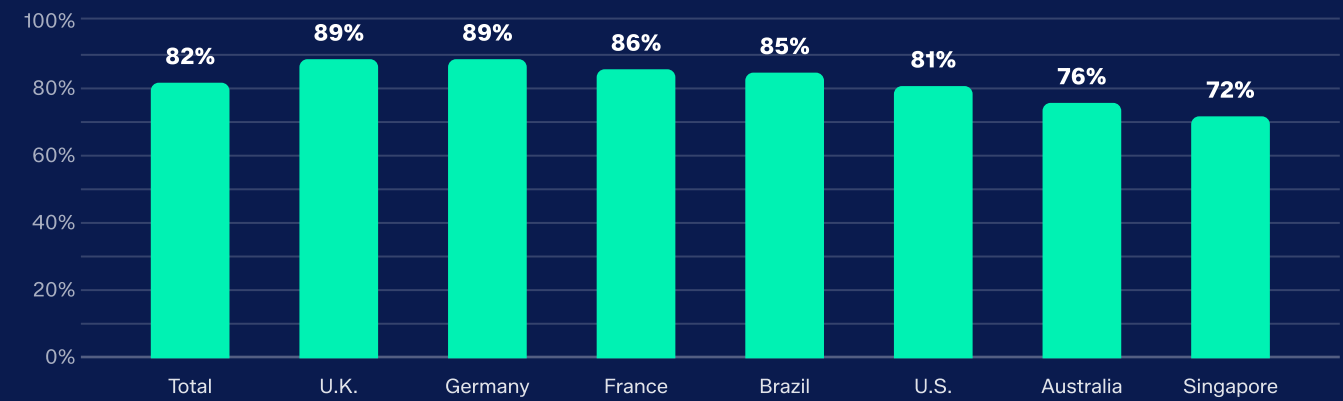
33%

are “completely confident” in their ability.

Confidence in managing compliance and control gaps varies by country

While managing compliance and control gaps is a well-established capability for most MSPs, confidence varies by country. MSPs in the U.K. and Germany say they are most likely to both easily identify and remediate these (89%), compared with 81% in the U.S., 76% in Australia, and 72% in Singapore. These differences suggest that while many providers have operational processes in place, the practical challenge of maintaining compliance and reducing risk is greater in some markets than others.

Ease of identifying and remediating compliance gaps varies by country



How easy or difficult is it for your organization to identify and remediate compliance or control gaps for your customers today? (n=800)

MSPs of all sizes are confident in their ability to manage customer compliance continuously

Confidence levels are remarkably consistent across MSPs of all sizes. Smaller providers report the highest overall confidence, with **98% of MSPs** with 1-5 employees saying they are "completely" or "very" confident in their ability to manage continuous compliance, compared with **92%** of MSPs with 51 or more employees. Complete confidence remains much lower across every size band, ranging from **30% to 36%**. The gap between high confidence and complete certainty suggests that while continuous compliance capabilities are becoming established across the MSP community, many providers would benefit from improvements to their current model.

CONFIDENCE IN MANAGING CONTINUOUS COMPLIANCE	TOTAL	1-5 EMPLOYEES	6-25 EMPLOYEES	26-50 EMPLOYEES	51+ EMPLOYEES
Completely confident	33%	36%	34%	30%	31%
Very confident	62%	62%	62%	65%	60%
Not very confident	4%	2%	4%	5%	7%
Not at all confident	0%	0%	0%	1%	1%
Completely or very	95%	98%	96%	95%	92%

How confident are you in your organization's current ability to continuously monitor, manage, and document compliance requirements across multiple customers, if at all? (n=800)

Cyber resilience depends on the ongoing proof of compliance rather than periodic reassurance. For customers, that means clear evidence that controls are working, gaps are surfaced, and improvements are being made over time. MSP confidence shows this capability is clearly emerging, but a lack of complete certainty highlights both opportunities and risks. Providers who can step into the gap to provide consistent, scalable, and repeatable compliance services will be strongly positioned to expand into higher-value governance services. Those that cannot may struggle to provide the level of assurance customers need as threats, regulations, and business risks continue to intensify.

Part 3: Operationalizing security and compliance at scale

1. Tool-based delivery is the standard

As MSPs expand their role in cybersecurity compliance and strategic advisory services, tool-based delivery has become standard practice. **89% of MSPs** now use one or more tools or platforms to centrally manage compliance or CISO-type activities across their customer base. Just **9%** continue to rely on entirely manual processes, while **2%** don't offer these services at all.

Adoption of these operational technologies has not led to widespread consolidation. More MSPs use multiple tools or platforms (**53%**) than a single solution (**36%**), suggesting that many are delivering these services through a collection of specialized platforms rather than a single, unified system.

This potentially reflects the growing complexity of managing compliance requirements, risk assessments, reporting, governance activities, and customer communications at scale. It also highlights a common challenge: many tools cannot feed data into a central reporting platform, creating the need for manual effort to consolidate activities into a single customer-facing report. The findings suggest growing demand for more unified approaches to managing and reporting on compliance programs.

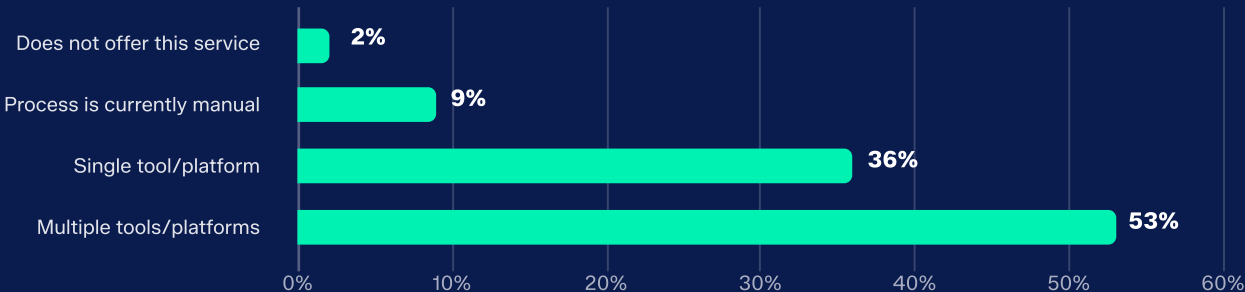
53%

of MSPs use multiple tools or platforms to centrally manage cybersecurity compliance or CISO-type activities.

36%

of MSPs rely on just one tool or platform

Platform approach to compliance/CISO activity delivery

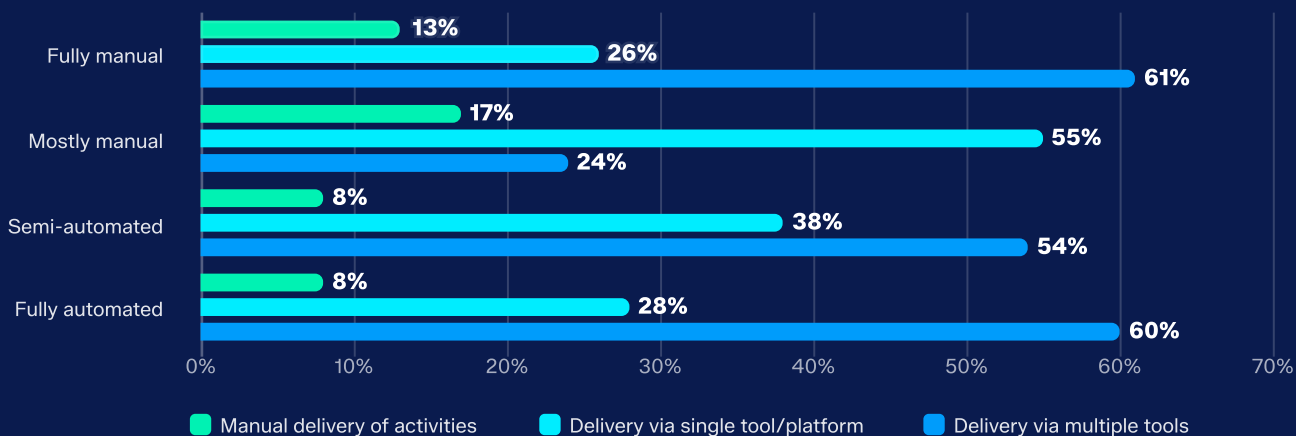


What approach does your organization currently use to deliver cybersecurity compliance or CISO-type activities across your customer base? (n=800)

2. Security reporting is becoming automated

Most MSPs have moved away from fully manual reporting processes, with **86%** using either fully automated or semi-automated methods to produce consolidated security posture reports. However, complete automation has not been normalized. Just **31% of MSPs** can generate reports quickly through a fully automated process, while **55%** still rely on some manual effort to combine data, add context, and finalize reports.

Reporting automation level by delivery approach



What approach does your organization currently use to deliver cybersecurity compliance or CISO-type activities across your customer base vs how automated is your organization's process for producing consolidated security posture reports for customers that show cybersecurity status, risks, and recommendations (n=800)

This shows that platform strategy alone does not equal automation maturity; MSPs at all levels of automation are using multiple tools, which may result from process fragmentation or the presence of more automated workflows across a broader toolset. Either way, the need for automation and the value it can create for MSPs is widespread.

86%

of MSPs use a fully or semi-automated process for producing consolidated security posture reports.

31%

can generate reports quickly with the support of automation.

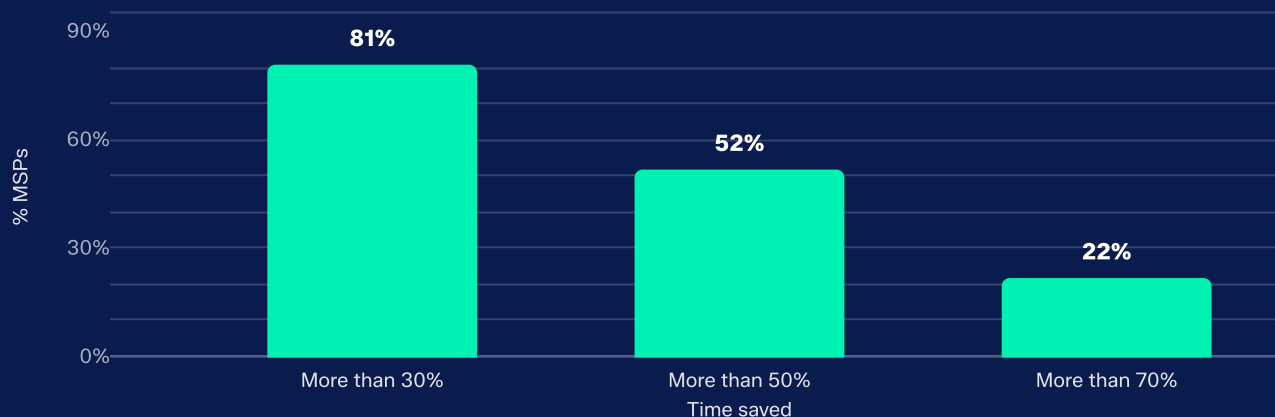
55%

still require some manual effort to consolidate activities.

3. Significant efficiency gains remain untapped

Platform consolidation could deliver substantial efficiency gains for MSPs. On average, MSPs estimate that a single, fully unified platform could reduce the time their teams spend managing and reporting on customer security posture and compliance by **53%**. Overall, **81% of MSPs** anticipate time savings of more than **30%**, 52% more than 50%, and 22% more than 70%.

Estimated time savings from a unified platform



What proportion of your team's time could be saved if all customer security posture and compliance management and reporting were handled through a single, fully unified platform? (n=800)

Perceived savings are particularly high among MSPs already delivering full compliance program management; **84% of MSPs** offering this service say they could create more than **30%** in time savings, compared to **64%** among MSPs that neither offer nor plan to offer the service. This suggests that those managing more comprehensive or integrated compliance activities may have the most to gain from platform consolidation.

These findings highlight the operational burden many MSPs still face when managing reporting, compliance, and advisory services across multiple platforms and workflows. As demand for higher-value services such as compliance management and CISO-style guidance grows, identifying ways to re-architect cyber program management at scale is becoming essential.

The results suggest MSPs see significant value in using a unified model to bring together the complete compliance program, helping their teams spend less time consolidating information and more time delivering strategic outcomes for their customers.

53%

the time MSPs would save if customer security posture and compliance management and reporting activities were handled via a single, unified platform.

81%

of MSPs say that unified approach would save more than 30% of their team's time.

22%

say they would save more than 70% of that time.

Conclusion

The MSP landscape is undergoing a significant shift. Customers increasingly expect their providers to deliver strategic cybersecurity leadership alongside technology management. MSPs are responding by expanding into compliance management, cyber advisory services, and other CISO-style roles. With **84% of surveyed MSPs expecting demand for CISO services to increase over the next year**, these higher-value services represent a growing opportunity for business growth and differentiation.

At the same time, managing security posture, compliance, and customer reporting at scale remains operationally challenging. While most MSPs have adopted platforms and automated processes, many still rely on multiple tools and manual effort to deliver these services. In many ways, this mirrors the complexity faced by CISOs and security teams, leaving MSPs grappling with the same challenges they are attempting to help their customers overcome.

MSPs that can reliably and efficiently deliver scalable cybersecurity leadership, continuous program management, and measurable security outcomes will be best positioned to strengthen customer relationships, grow sales, and capitalize on the next frontier of opportunities.

Sophos CISO Advantage

[Sophos CISO Advantage](#) provides the opportunity for MSPs to lead a different kind of cybersecurity conversation: one focused on outcomes, business risk, progressive compliance, and measurable improvement.

Delivered through [Sophos Fusion](#), the Sophos AI-Native Cybersecurity Defense System, it transforms the CISO role most MSPs are already delivering into a structured, scalable, billable cyber program management service.

Agentic AI-accelerated assessment, reporting, and roadmap workflows give these essential partners a repeatable way to deliver board-ready insight, framework-mapped evidence, and prioritized action plans across their customer base.

It also creates a clear route into new recurring revenue, growth opportunities, and stronger customer relationships from within engagements. Every assessment surfaces security gaps and every gap opens up a roadmap for improvement, positioning MSPs to deliver those follow-on solutions.

Sophos CISO Advantage responds to a demand the security community has been highlighting for years. By becoming early adopters, MSPs can fully step into the leadership role their customers so evidently need them to provide.

To learn more about Sophos CISO Advantage, MSPs can visit the [Partner Portal](#).

Want to become a Sophos Partner? **Register here.**

United Kingdom and Worldwide Sales

Tel: +44 (0)8447 671131

Email: sales@sophos.com

North America Sales

Toll Free: 1-866-866-2802

Email: nasales@sophos.com

Australia and New Zealand Sales

Tel: +61 2 9409 9100

Email: sales@sophos.com.au

Asia Sales

Tel: +65 62244168

Email: salesasia@sophos.com