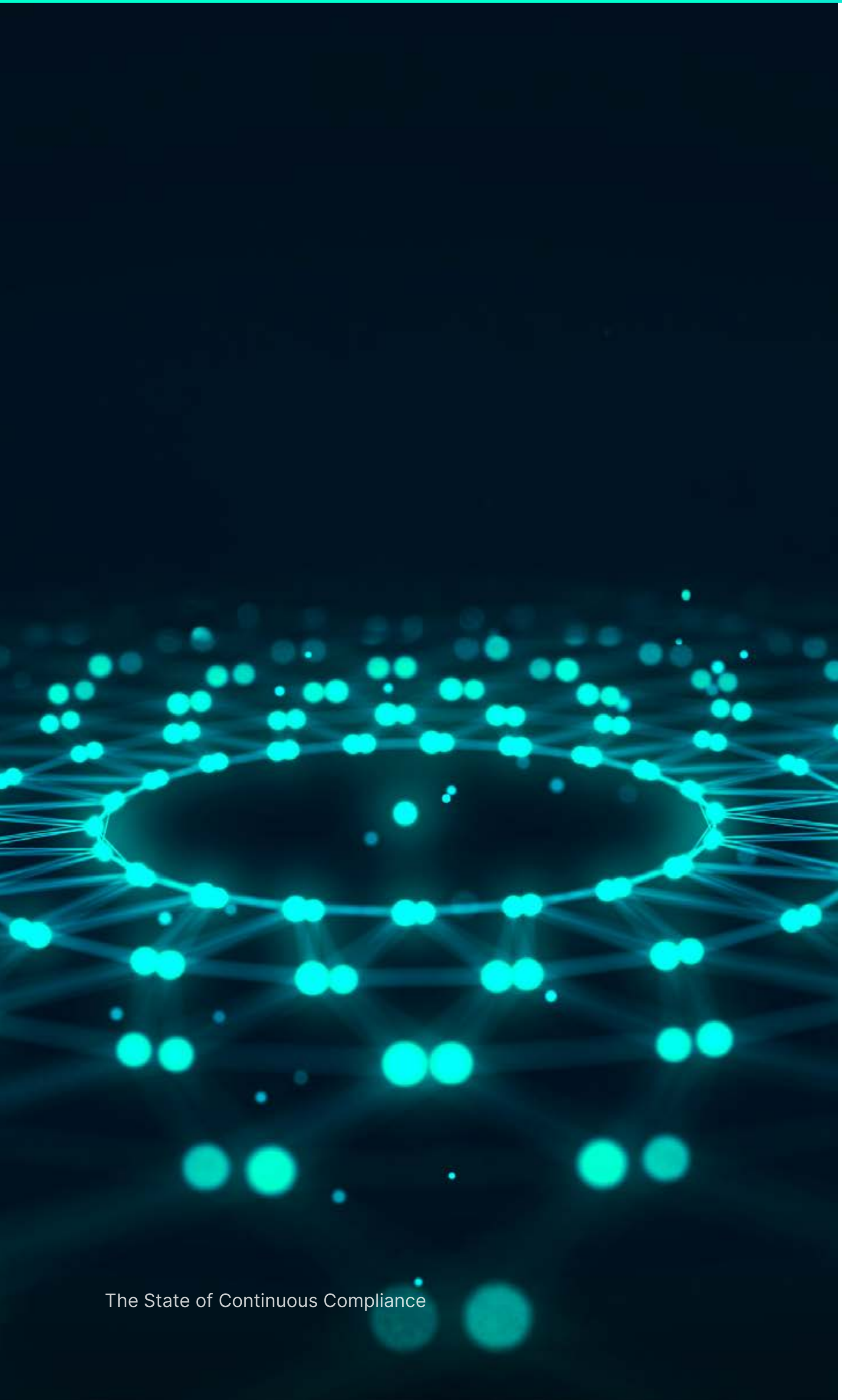
Apptega

REPORT

The State of Continuous Compliance

2024

Contents



Executive Summary

Let's get this out of the way: Compliance is not a sexy topic. So I preface the findings of Apptega's inaugural State of Continuous Compliance Report with a knowing admission: The conclusions herein better make a compelling case for you to care.

They do.

They do, that is, if you're among the many managed security providers navigating the rapidly evolving business landscape of 2024 — facing challenges growing, headwinds differentiating, stiffening competition, and difficulty retaining increasingly flakey customers.

Detailed responses from hundreds of security providers ranging from 10-person consultancies to among the largest and most respected MDR companies in the world paint a clear picture: In a cut-throat environment where recurring revenue and margin growth are at a premium, continuous compliance services represent a massive, and massively lucrative, opportunity—and one going largely unmet due to lack of expertise, resources, and capable tooling.

Specifically, of the more than 70% of providers facing double-digit annual revenue growth expectations, four in five view compliance as a high-growth business segment—but fewer than half of all providers currently offer managed compliance services.

Continuous compliance—I and many within the Apptega partner ecosystem believe—represents a powerful source of business for a large swath of managed security and service providers that find themselves at a crossroads. On the one hand, many have enjoyed years of seemingly unfettered growth as organizations have invested heavily in security and digital transformation. On the other, in 2024, there is ample evidence to suggest that the “golden era,” as one industry observer appropriately put it, is slowly coming to an end.

We appear now to be entering a phase of consolidation, unprecedented M&A, and private equity-backed rollup where only the strong balance sheets will survive and only the differentiated will thrive—or successfully exit.

To be sure, the emergence of continuous compliance, or compliance as a service, is but one of many onramps to the type of recurring revenue that investors and potential acquirers find so attractive. But its applications, as the regulatory and risk landscapes intensify, go beyond mere box checking.

Increasingly, as this report will show, providers are effectively positioning compliance both as a standalone offering and as a “tip of the spear” for high-margin security bundles: a way, yes, to assess and show whether clients meet requirements, but also as a way to justify the cost, and validate the ROI, of the security services they deploy that go toward fulfilling those controls.

Still, as the following pages describe, there is much work to be done to fill the knowledge, technology, and resource gaps that must be overcome to fully capitalize on this enormous opportunity. We’ll be heads down doing our part. We commend you for doing yours.

Dave Colesante
Apptega CEO

Purpose and Scope

Compliance work is often highly manual, specialized, and resource intensive. Many providers lack the tools to deliver or conceptualize products and services to meet client compliance needs. And the work is traditionally made up of one-off gap or risk assessments that contribute only temporary revenue, so it’s harder for providers to achieve their growth goals.

The aim of this inaugural State of Continuous Compliance Report is to better define, understand, and benchmark these challenges, helping clear the hurdles to progress so providers can maximize growth and stand out among stiff competition.

To that end, Apptega surveyed practice leaders and senior operators at 115 security providers from March to May of 2024. The data in this report summarizes responses across segments and provides general takeaways.

While this report is not conclusive, it does provide a relevant snapshot of the compliance trends, challenges, and opportunities that providers face today. With first-of-its-kind compliance benchmarking data specifically for providers, this report is a guide to improving business growth and revenue in a competitive market.

The report will cover:

- How (and if) providers are delivering compliance today and structuring their compliance offerings.
- The challenges they face in maintaining or offering compliance services.
- The difference between those using compliance technology and those that are not.
- How continuous compliance can help service providers improve recurring revenue (as measured by ARR or MRR), efficiency/bandwidth, and their ability to differentiate.
- And what the prospect of continuous compliance means for providers and their customers.

Key Findings & Takeaways

Revenue & Growth

- ✓ 3 out of 4 respondents view compliance as a “high growth” business.
- ✓ 86% of respondents have a strong desire to turn one-off projects into recurring revenue.
- ✓ 70% of respondents have at least double-digit revenue growth targets.

Takeaways

- ✓ Managed service and security providers face aggressive business growth expectations.
- ✓ A large majority view compliance as a high-growth opportunity.
- ✓ Most providers don’t offer managed compliance due to a lack of resources, expertise, or technology.
- ✓ Providers that offer managed compliance are more optimistic about revenue growth, efficiency, and outcomes.

15%

offer compliance primarily as a managed service.

85%

face “significant challenges” maintaining compliance for customers.

50%

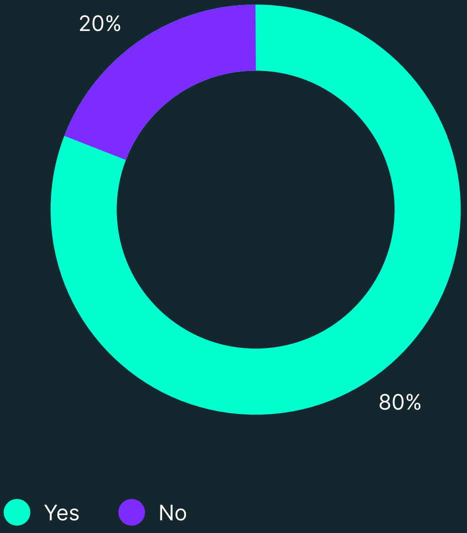
use spreadsheets to track customer compliance.

The State of Compliance Today

The primary goal of this State of Continuous Compliance Report is to uncover how managed service and security providers deliver cybersecurity compliance today. This section examines how they package compliance services as part of their complete business offering.

Overall, **80% of the surveyed providers offer some form of compliance services (Figure 1).** While this indicates that the overwhelming majority see value in compliance for their clients, a much smaller percentage is capitalizing on the full opportunity, as we examine in the following pages.

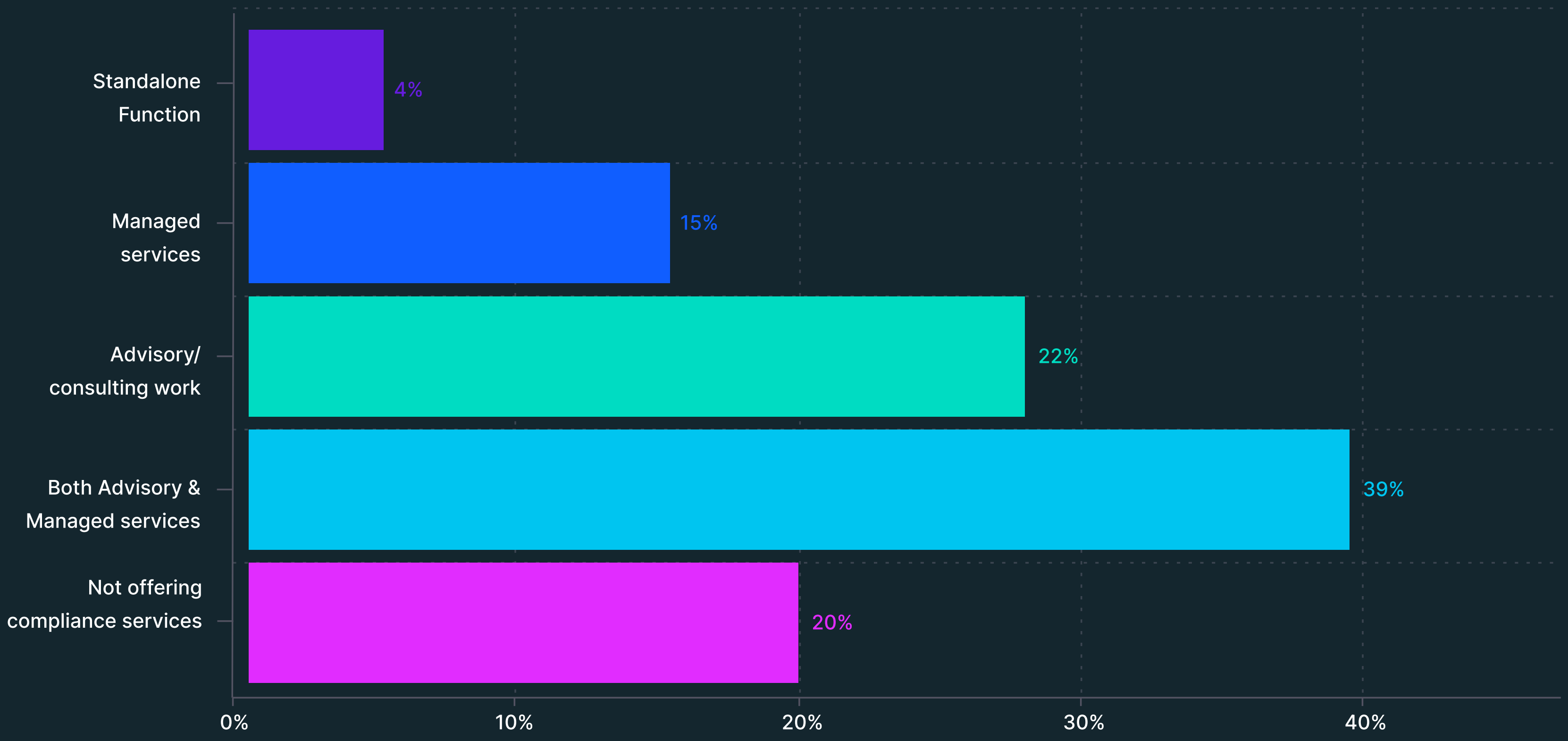
Percentage of security providers offering compliance services (fig 1)



Providers Have a Managed Compliance Gap

Providers are leaving opportunities on the table when it comes to their compliance services. **Many only offer compliance in an advisory capacity, outpacing compliance as part of managed services by 38% (Figure 2).** While 39% offer compliance through a mix of the two practices, only 15% of compliance practices live primarily on the managed services side compared to 22% for advisory/consulting work.

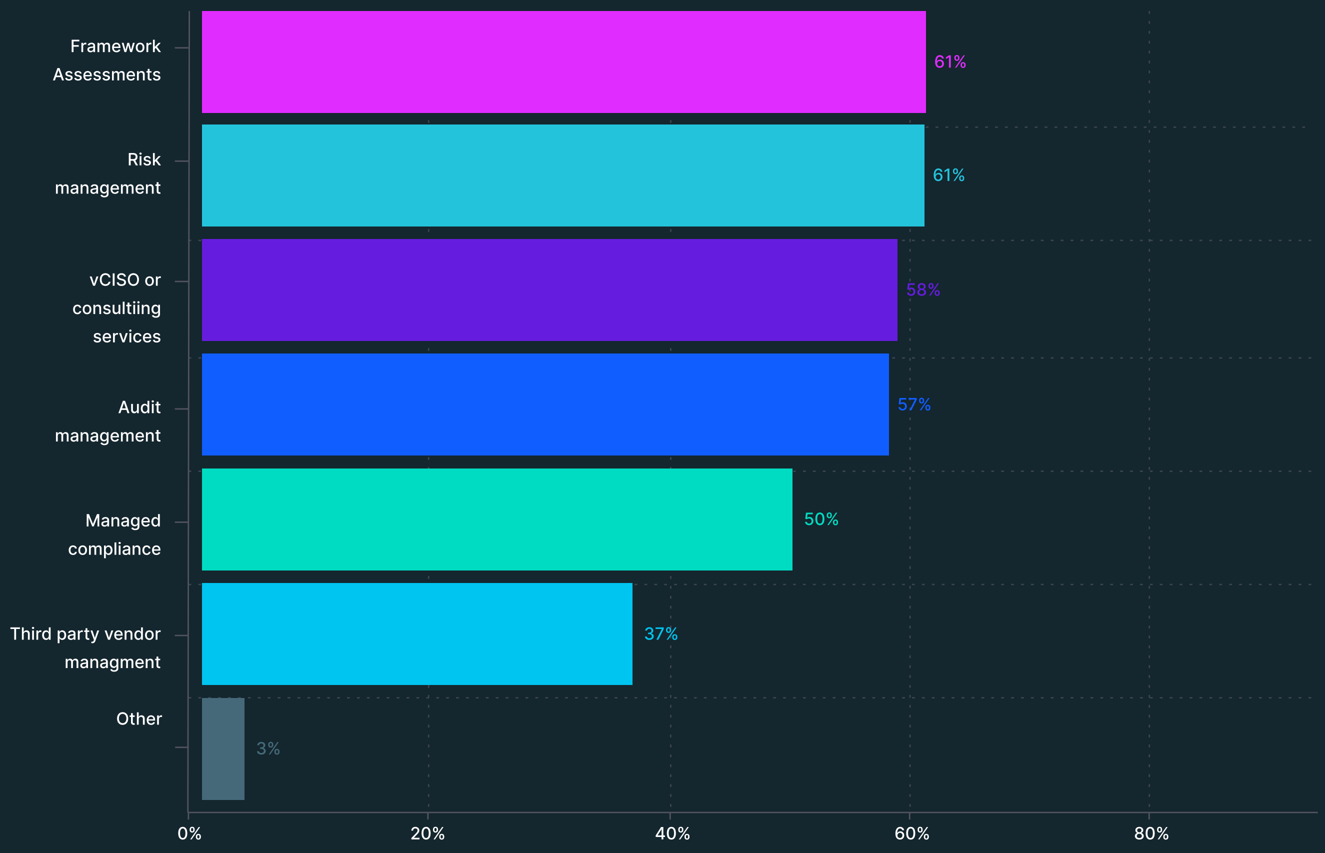
Compliance by business segment (fig 2)



Looking at individual services rendered within the different practices, managed compliance makes up a smaller percentage of the total compliance portfolio. **Only half of all providers offer managed compliance as a service (Figure 3).** Framework assessments (61%), risk management (61%), vCISO or consulting services (58%), and audit prep/management (57%) were all offered at a rate significantly higher than managed compliance.

Considering nearly three quarters of respondents view compliance as an area of high growth and 86% are interested in continuous compliance for their clients (Figure 7), there appears to be a gap between the opportunity providers see and their ability to fill it.

Compliance by individual services rendered (fig 3)



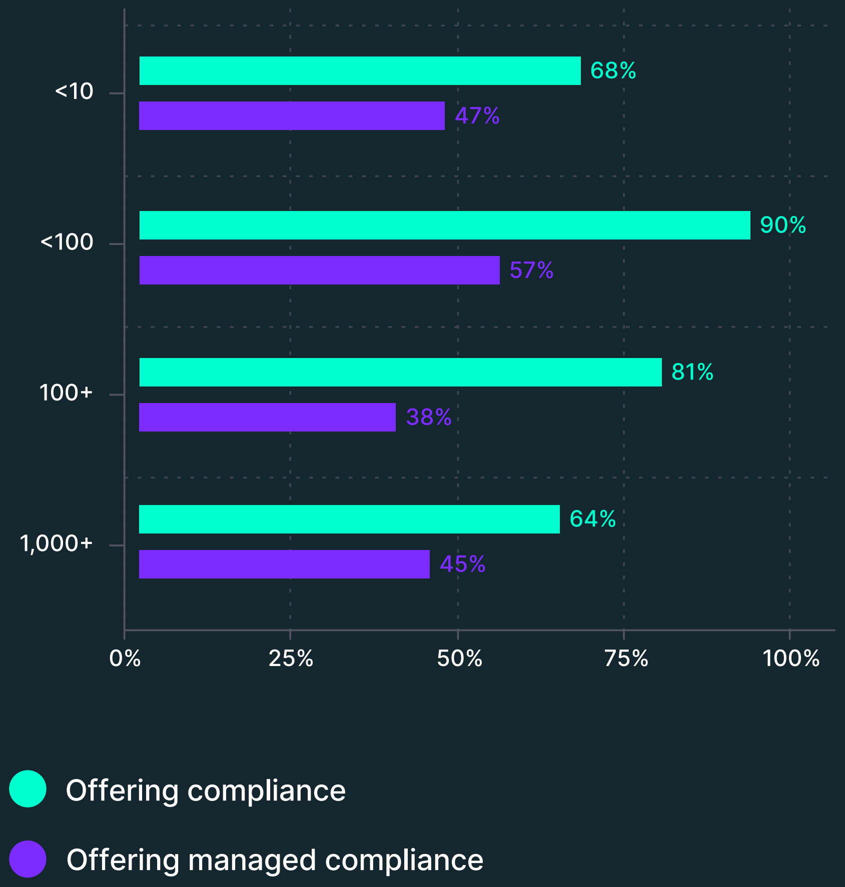
Smaller Providers Are More Likely to Offer Compliance Services

While it can be difficult to compete with larger security providers, compliance seems to be an area where smaller competitors are making up some ground.

Providers with fewer than 100 employees offer compliance at a rate 8% higher than those with more than 100 employees **(Figure 4)**. And they outnumber the larger providers by 26% for managed compliance services.

Looking at only the smallest and largest segments, providers with fewer than 10 employees and those with more than 1,000 offer compliance services at a similar rate. Those in the 10–99 employee range were the most likely to offer compliance and managed compliance services.

Compliance by employee count (fig 4)



Compliance Packaging Presents Opportunity to Differentiate

Providers package their compliance offerings in three main ways. The first is by aligning to security best practices— but not necessarily against a standardized best practice framework. These organizations may use compliance frameworks as a proxy for best practices, proof point for success, or method for gauging security posture, but they aren't providing formal compliance offerings. Of the providers offering some form of compliance, only 7% take this approach.

Like the nearly 20% that aren't offering any compliance services, these providers could be overlooking a valuable piece of the market. They're likely already delivering services that address compliance requirements in some way, but by not packaging these services as a formal compliance offering, they could be limiting their business.

> I think some of these service providers are missing an opportunity to go after a market they already solve for through their security offerings.
>
> Their clients don't have the people, time, or budget to manage compliance, so they're going through consultants for their audits, paying higher consulting fees.
>
> A formal compliance offering improves a provider's value prop, making it more relatable to the customer. It's an opportunity to boost revenue and value through more holistic offerings, and they're already providing some of the services.
>
> **Rahul Bakshi**
> Chief Product Officer, Apptega

Many providers offer compliance via a la carte services that address key framework controls, including network detection, vulnerability management, and Log/SIEM detection. Nearly half of providers package their compliance offerings in this way. While this approach provides a more formal compliance offering, and helps providers validate the effectiveness and ROI of their security services, they could still be leaving value on the table compared to the next option.

Framework-based offerings or bundles make up 46% of compliance packages. By bundling the entire end-to-end compliance program and managing it through a technology platform, it appears providers are creating a broader offering that delivers greater value, recurring revenue, and customer stickiness.

With less than half of providers bundling compliance services, there’s a large opportunity to differentiate and improve recurring revenue.

7%

align offerings to security best practices.

47%

offer services a la carte depending on client need.

46%

use framework-based offerings/bundles.

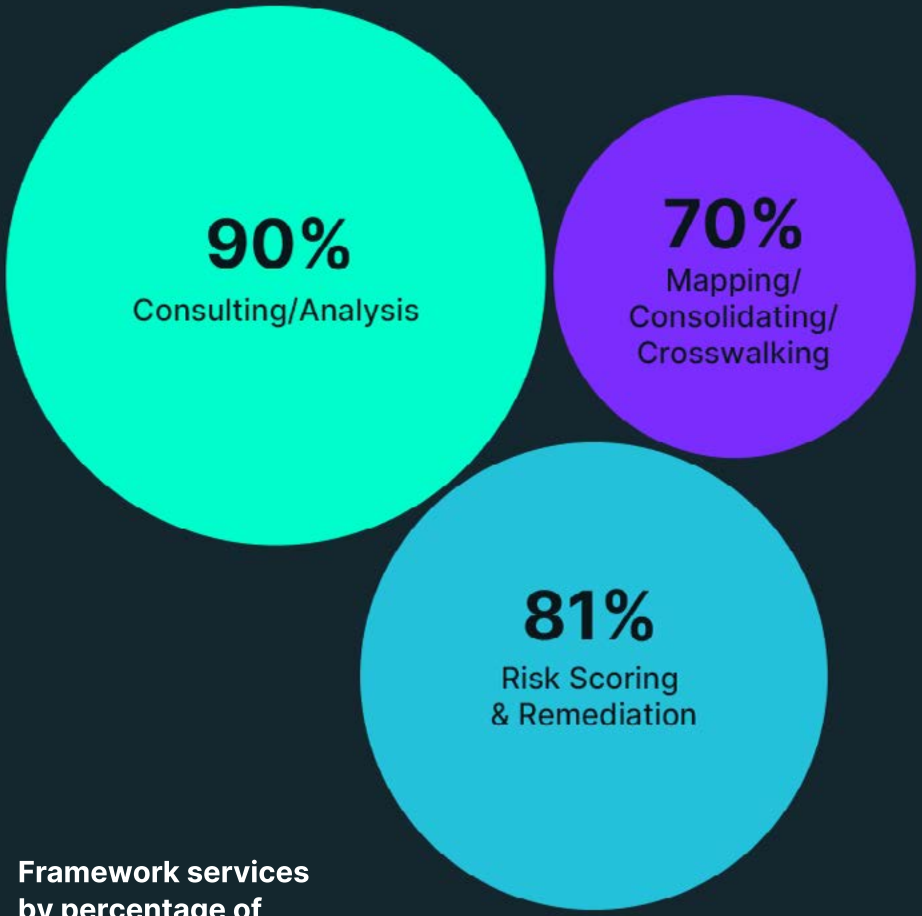
More Than Half of All Providers Lack Framework Crosswalking

Cybersecurity frameworks are a crucial tool for helping organizations evaluate their security postures and meet compliance standards and regulations.

But nearly 40% of respondents said they don't offer framework-based services. Of the ones who do, 90% are providing consulting and analysis, 81% provide risk scoring and remediation, and 70% are providing framework mapping, consolidation, and crosswalking—mapping controls in one framework to similar controls in others **(Figure 5)**.

While all these services are valuable, the latter potentially presents the best opportunity for providers to differentiate. With many organizations managing multiple frameworks, mapping common controls across them can save time, money, and help avoid duplicative work.

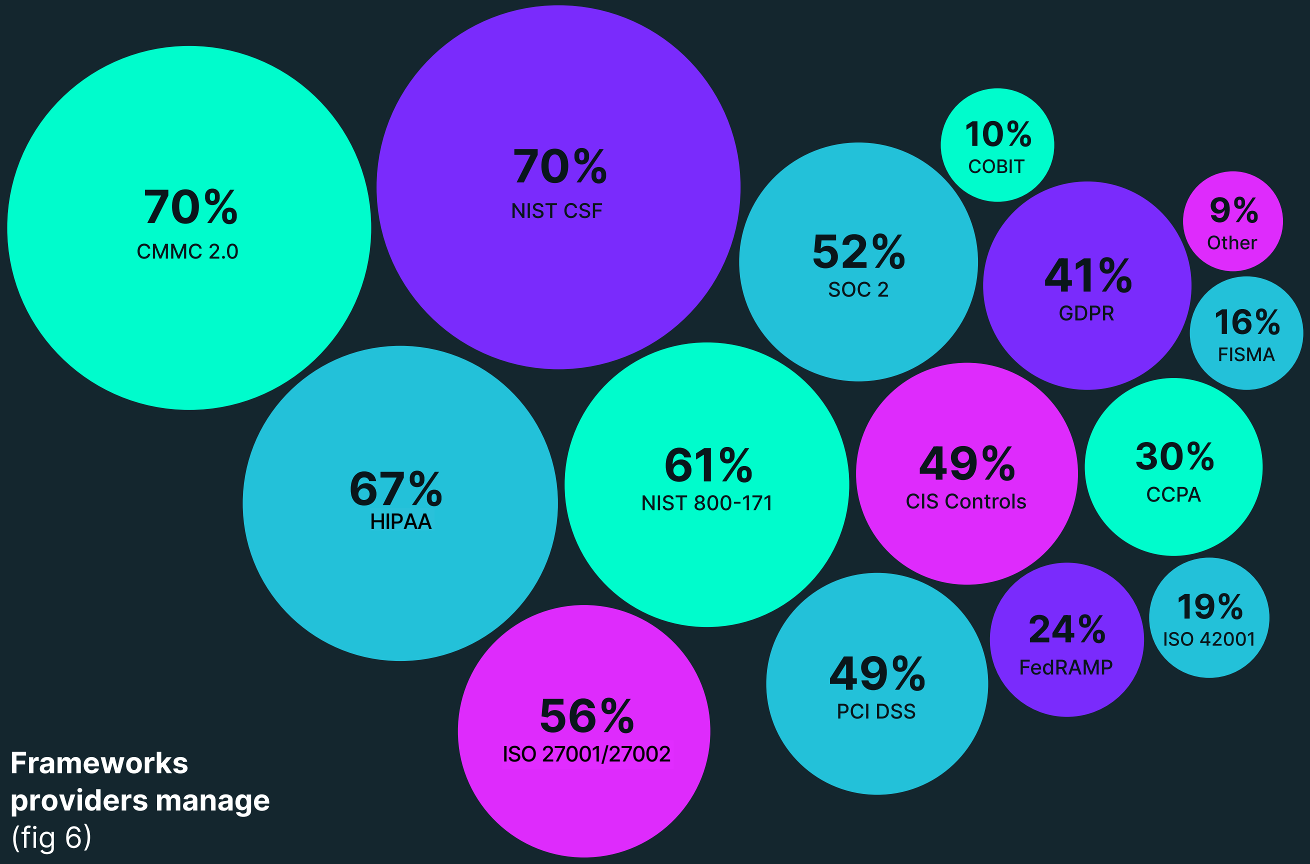
Framework crosswalking creates new service opportunities for providers and helps them stand out from 58% of the total competition that isn't offering these services.



Framework services by percentage of providers
(fig 5)

Least-Offered Frameworks Provide Potential Opportunities

Providers are tasked with helping clients meet requirements for several frameworks. The most common among the 61% of providers offering these services include CMMC, HIPAA, and NIST 800-171 **(Figure 6)**. Given the highly regulated nature of government and healthcare work, these results aren't surprising. But some of the least-offered frameworks provide potential opportunities for providers, such as ISO 42001—the new artificial intelligence management system standard—which will likely grow in reach and is currently managed by only 19% of providers offering framework services (12% of all providers).

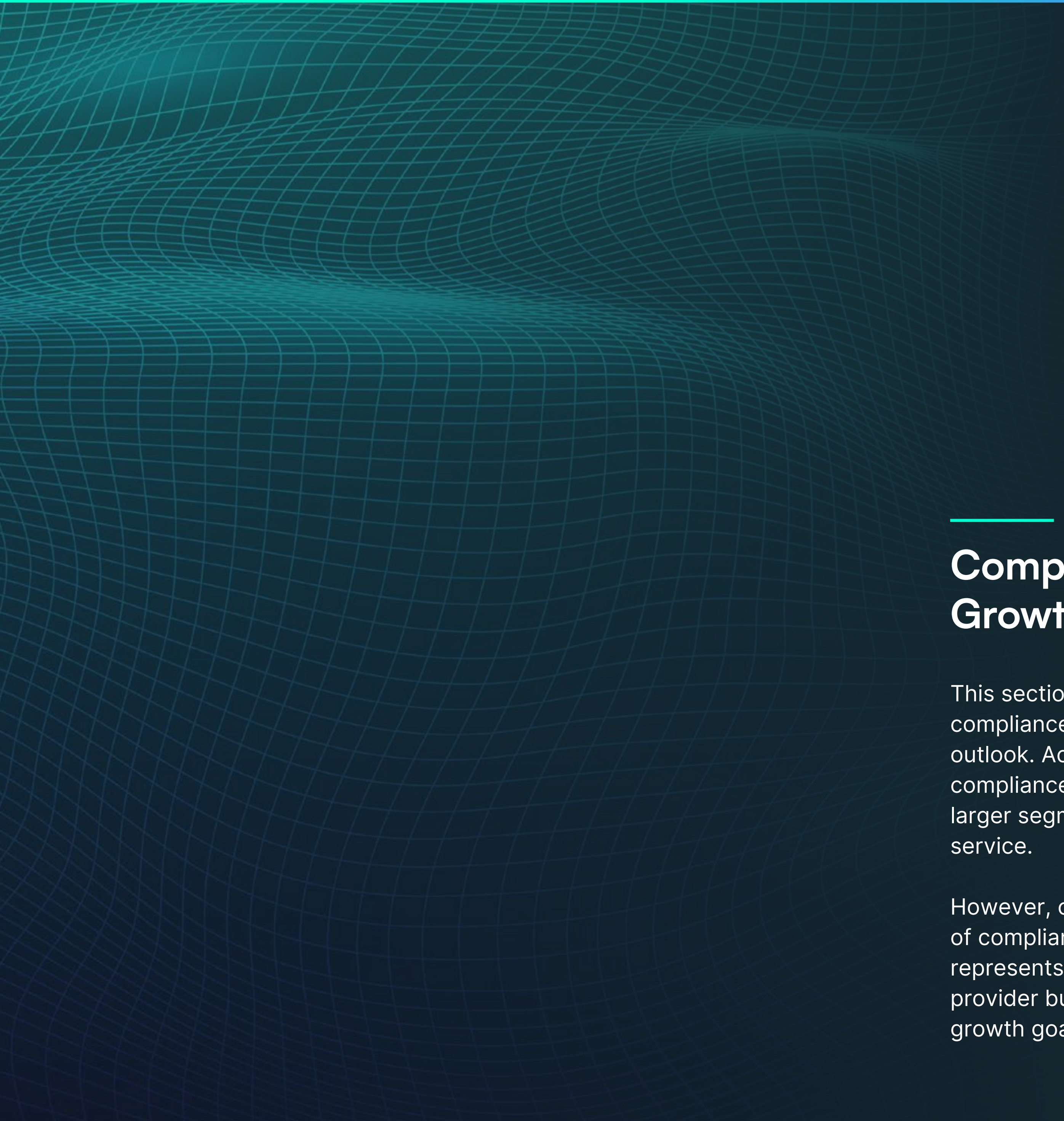


Frameworks providers manage
(fig 6)

CyberSecOp

“Clearly, managed compliance represents a lucrative opportunity for the relative few services and security providers equipped to offer it. Unfortunately, most lack the technology, resources, and know-how to deliver an impactful assessment and follow-on program. At CyberSecOp, we’ve partnered with Apptega to go to market with a differentiated continuous compliance offering that allows our world-class security expertise to shine.”

Chris Yula
VP of Sales & Strategy, CyberSecOp



Compliance Revenue and Growth Potential

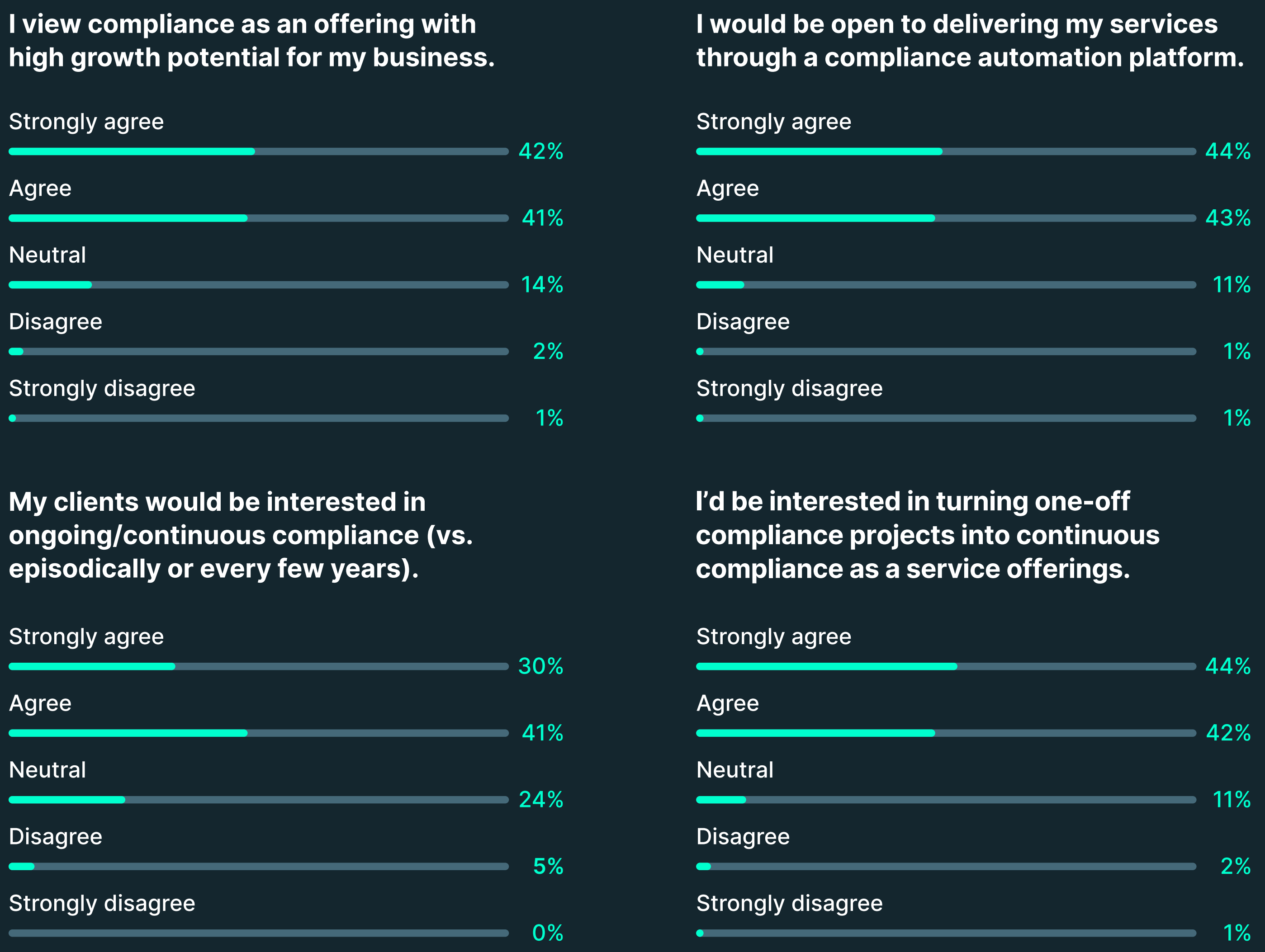
This section explores the value of continuous compliance in terms of its revenue and growth outlook. According to the data, most providers view compliance as an area of high growth. And an even larger segment sees the value of compliance as a service.

However, continuous compliance, the delivery of compliance services on an ongoing basis, represents a disproportionally small percentage of provider business and revenue, despite aggressive growth goals.

Providers View Compliance as a High-Growth Opportunity

Nearly 3 out of 4 providers (74%) view compliance as an area of high growth, including those that aren't currently offering compliance services. Among providers that are already offering some form of compliance, more than 4 out of 5 (83%) agree or strongly agree that it has high growth potential **(Figure 7)**.

Compliance growth potential for providers offering compliance services (fig 7)



I view compliance as an offering with high growth potential for my business.

I would be open to delivering my services through a compliance automation platform.

My clients would be interested in ongoing/continuous compliance (vs. episodically or every few years).

I'd be interested in turning one-off compliance projects into continuous compliance as a service offerings.

Providers and Their Clients Want Continuous Compliance

Compliance work is typically made up of one-off engagements that provide limited recurring revenue potential. To remove that barrier to growth, **86% of providers offering compliance services are interested in continuous compliance as a service offerings for their clients (Figure 7).**

According to 70% of these providers, their clients would also be interested in continuous compliance to ensure compliance and security monitoring and scoring around the clock, rather than just in the lead-up to audits.

Lastly, 87% would be open to delivering their services through a continuous compliance platform, with automated workflows and real-time visibility into compliance status.

What is continuous compliance?

Also known as ongoing or recurring compliance, continuous compliance is a proactive approach that helps turn one-off projects into long-term client relationships.

It transforms compliance from a check-the-box exercise into a continuous state of improvement and scoring, from assessment to audit-ready programs. With continuous compliance, providers can increase recurring revenue, expand margins, and improve customer retention.

Providers Have Ambitious Growth Goals, Limited Recurring Revenue

While providers recognize the benefits of continuous compliance and are interested in offering the service, these sentiments have not generally translated into revenue. Nearly half of providers receive less than 10% of their revenue from compliance services **(Figure 8)**. Only 1 out of 4 providers (26%) generate more than a quarter of their revenue from compliance services.

Only 36% receive more than half of their compliance revenue from recurring projects versus one-off engagements. For the majority (56% of providers), less than a quarter of their revenue is recurring.

Compliance revenue potential for providers offering compliance services (fig 8)

	0%	<10%	<25%	<50%	50%+	75%+	100%	Unsure
Overall revenue from compliance services	2%	47%	22%	8%	10%	9%	0%	2%
Recurring compliance revenue (vs. one-off payments)	8%	31%	18%	6%	10%	15%	11%	2%
Target ARR/MRR growth rate (YoY)	0%	18%	35%	15%	13%	3%	3%	12%

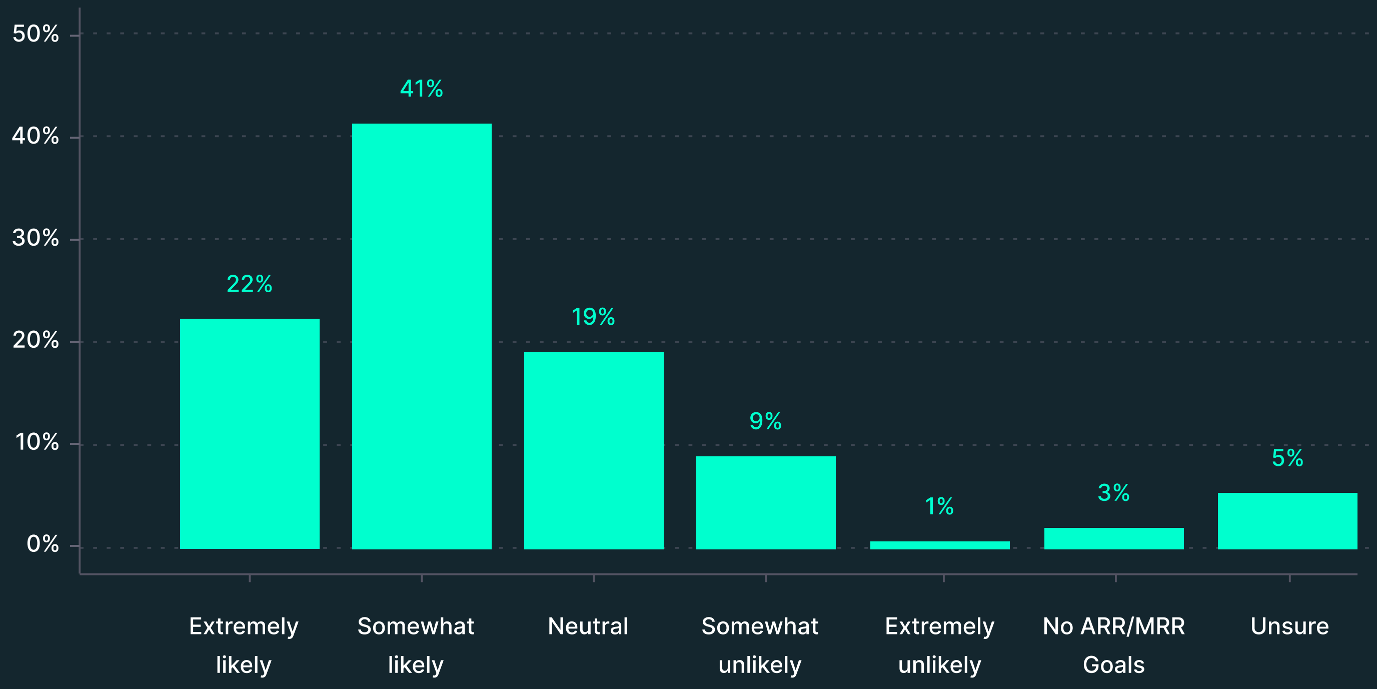
Security providers face aggressive business growth expectations, with 70% targeting at least double-digit ARR/MRR growth (Figure 8). Around 20% are targeting at least 50% growth.

While these growth goals are ambitious, 63% of providers say they're at least somewhat likely to hit them **(Figure 9)**. Only 10% believe they're unlikely to achieve their recurring revenue goals.

Given the overwhelmingly positive outlook around continuous compliance and compliance services in general—and the disproportionally low revenue coming from these services—there appears to be tremendous potential for additional growth.

If providers can increase recurring revenue through continuous compliance, they can more easily achieve their ambitious growth goals—or increase them even more.

Likelihood of hitting ARR/MRR goals (fig 9)

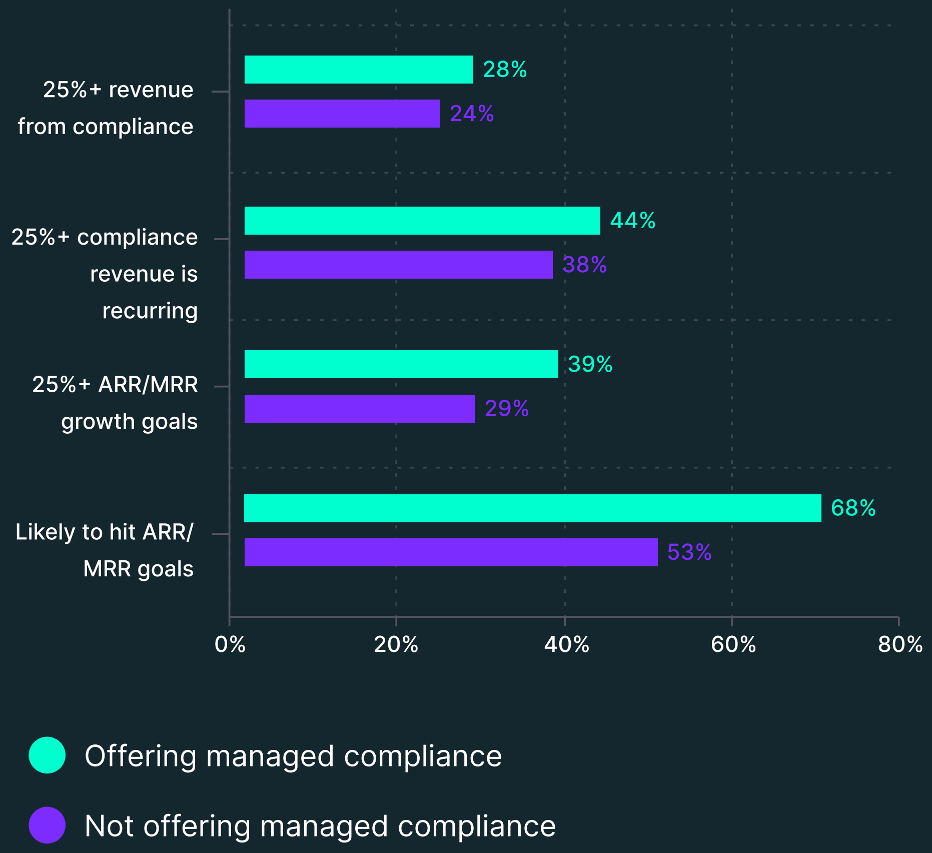


Providers Offering Managed Compliance Have Higher Revenue Growth Targets

Managed compliance provides a small boost to providers in terms of current and target revenue **(Figure 10)**. For those offering managed compliance services:

- 28% receive more than a quarter of their revenue from compliance services versus 24% for those not offering managed compliance.
- 44% get more than a quarter of their compliance revenue from recurring engagements versus 38%.
- 39% have target ARR/MRR growth of more than 25% versus 29%.
- 68% say they are likely to hit ARR/MRR growth goals versus 53%.

Current and target revenue:
Providers offering managed compliance vs. not (fig 10)



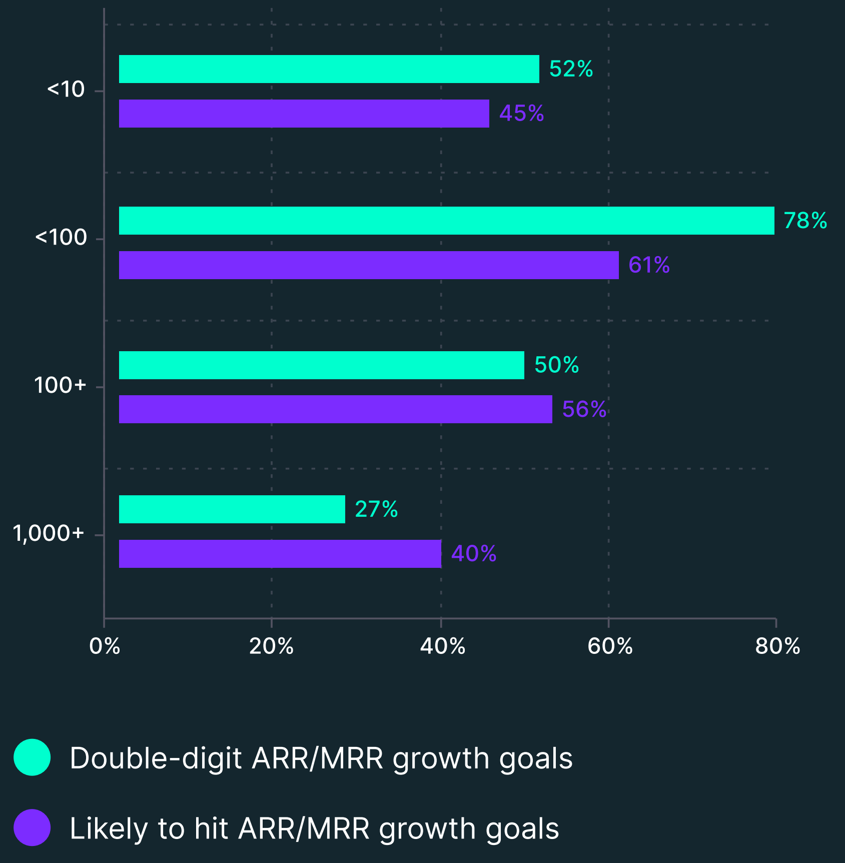
Smaller Providers Have Higher Growth Goals

Providers with fewer than 100 employees have more aggressive ARR/MRR growth goals than providers with more than 100 employees. Less than half of the larger companies (44%) have double-digit growth goals compared to 67% of the smaller ones **(Figure 11)**.

Similarly, half of the companies with more than 100 employees said they were likely to hit their ARR/MRR goals compared to 54% of the smaller ones.

While larger providers typically have lower growth expectations, their smaller peers face pressure to grow quickly. And with fewer large providers offering compliance services, smaller competitors have an opportunity to fill unmet demand.

ARR/MRR growth by company size (fig 11)



FORESITE CYBERSECURITY

“Compliance is an ongoing journey. You have to constantly manage, assess, and track it to make sure you achieve and maintain compliance. With continuous compliance, we’re giving clients that ongoing guidance and adding value. We’re taking one-off project revenue and making it recurring revenue over years. If you just sell them a tool with no guidance, they won’t renew. Clients stay with you when they see value.”

Tracy Fox
National Channel Sales Director,
Foresite Cybersecurity

The Challenges Limiting Providers

The previous section established that most providers view continuous compliance as a high-growth opportunity, but a smaller percentage is capitalizing on the potential to generate revenue. So, what's holding providers back?

This section explores the key challenges providers face when maintaining compliance for their clients. And they're the same challenges preventing 20% of providers from offering any compliance services at all:

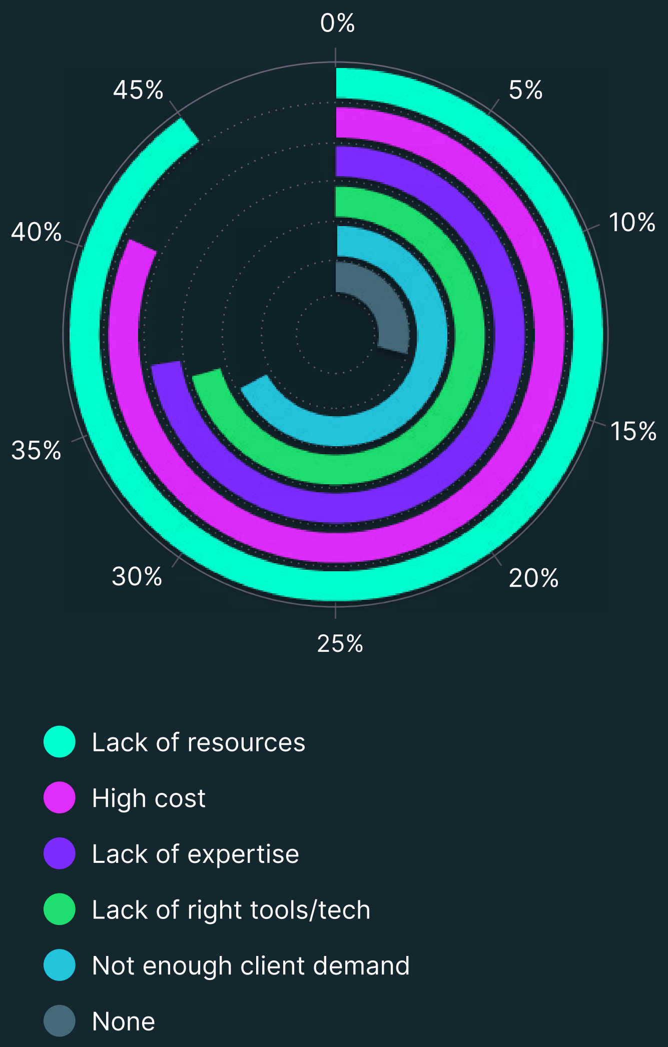
- High cost
- Lack of resources
- Lack of expertise
- Lack of the right tools/tech
- Not enough client demand

Providers Face Significant Challenges

Of the providers that offer compliance services, 85% face significant challenges maintaining compliance for their clients. The most common challenge is a lack of resources, which was reported by 45% of respondents **(Figure 12)**. Cost was next at 42% followed by lack of expertise (37%), lack of the right tools/tech (36%), and not enough client demand (34%).

> Many providers are missing out on a growing compliance market, but it's not because they don't see the potential value of these services.
>
> Providers must address a wide breadth of client challenges simultaneously and clearly demonstrate the value of often hard-to-quantify security services.
>
> Without the right tools, resources, and expertise, it becomes difficult to capitalize on the compliance opportunity. A robust compliance offering can help them overcome these challenges and meet aggressive growth mandates in an increasingly competitive space.
>
> **Dave Colesante**
> CEO, Apptega

Key challenges limiting compliance providers (fig 12)

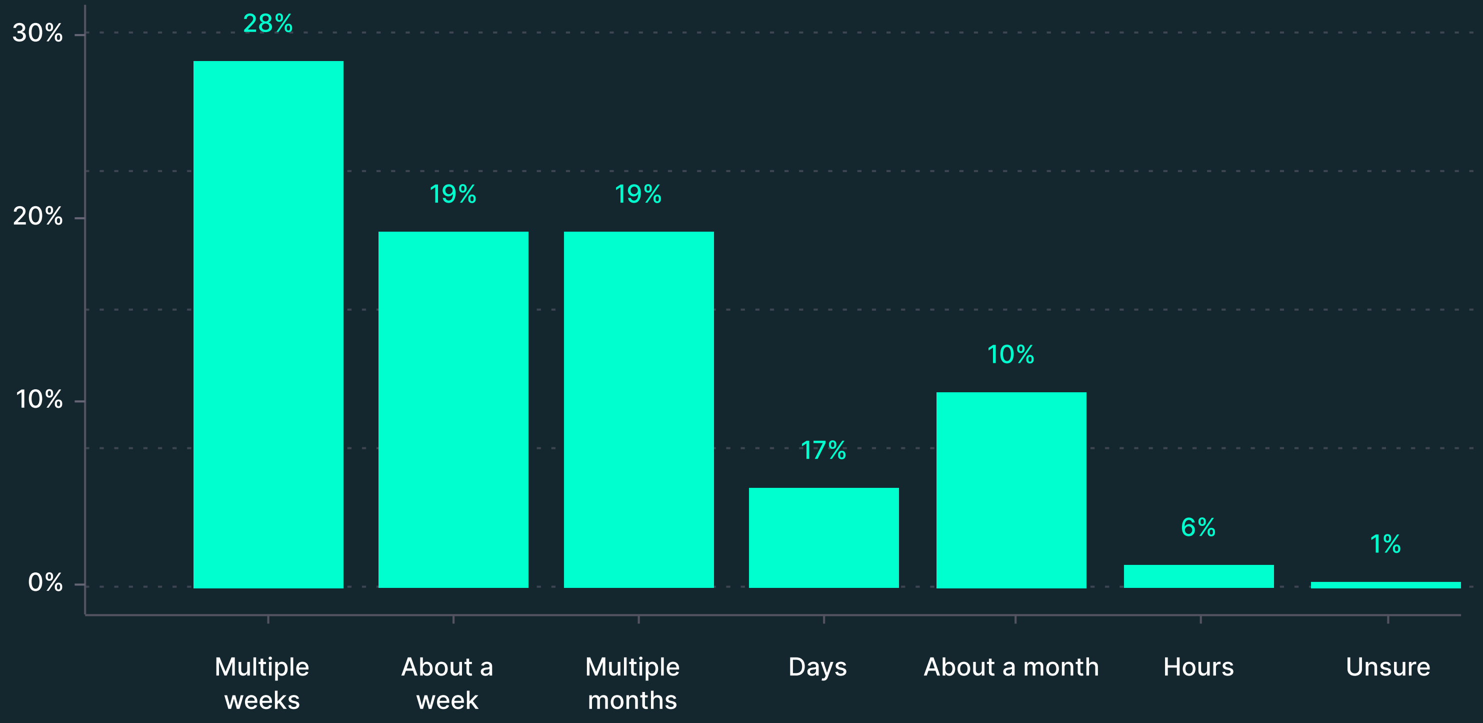


Risk Assessments Take Too Long

The challenges above trickle down into individual compliance services, creating additional problems. For example, of those providing risk or gap assessments, 75% say the process takes weeks or months when starting from scratch **(Figure 13)**. Only 23% say it takes hours or days.

With fewer resources and tools to fast-track the process, it takes many providers longer to complete assessments than it would with appropriate tools in place. In fact, 3 out of 4 providers who complete risk assessments in hours or days are using governance, risk, and compliance (GRC) software (31%) or a compliance automation platform (63%).

Time to complete risk assessments from scratch (fig 13)

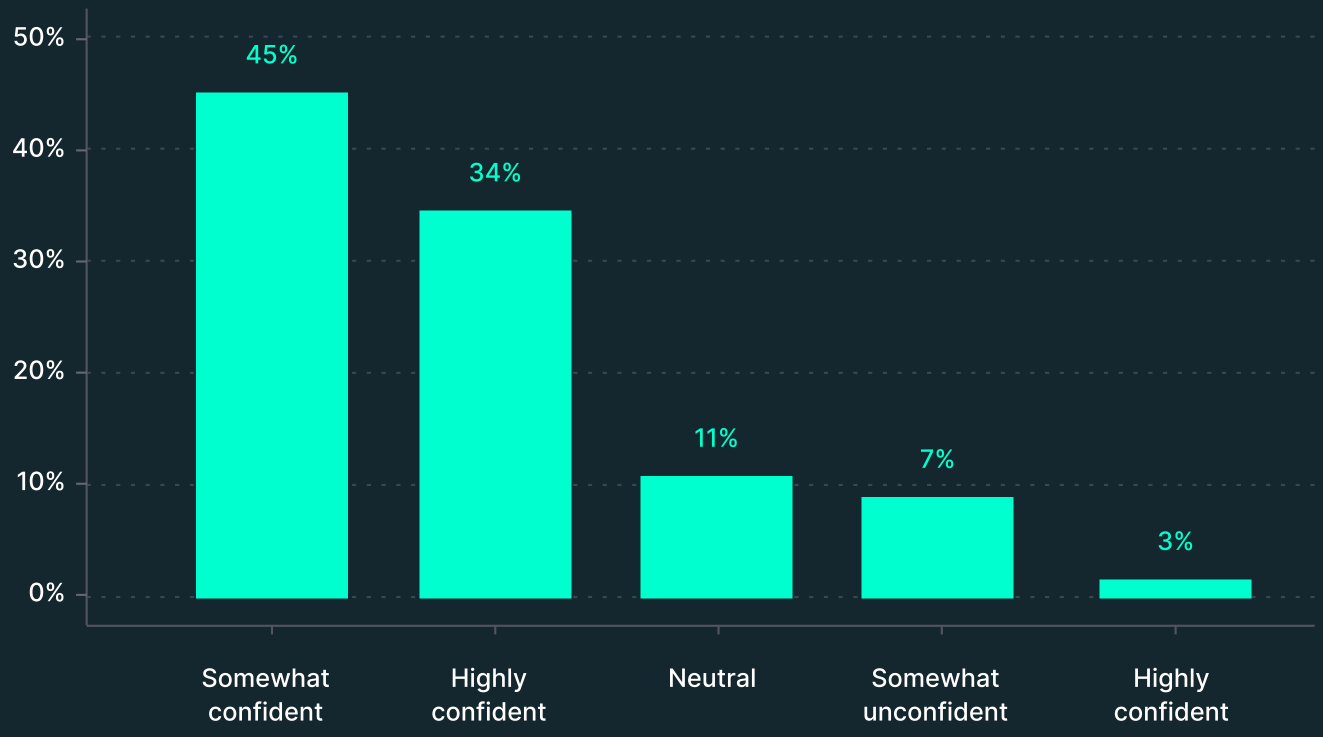


Providers Are Confident in Their Ability to Scale

Despite the challenges they face, if an additional 20% of their clients needed compliance services tomorrow, 79% of providers say they would be confident in their ability to scale quickly to meet demand **(Figure 14)**. Only 10% are unconfident.

This is somewhat surprising given that nearly 70% of the "confident" providers also reported either a lack of resources, lack of expertise, lack of the right tools/tech, or high costs—or a combination of these challenges. This suggests that while they may need to overcome challenges to scale, providers will allocate as necessary to meet client demand.

Provider confidence in ability to scale compliance services (fig 14)



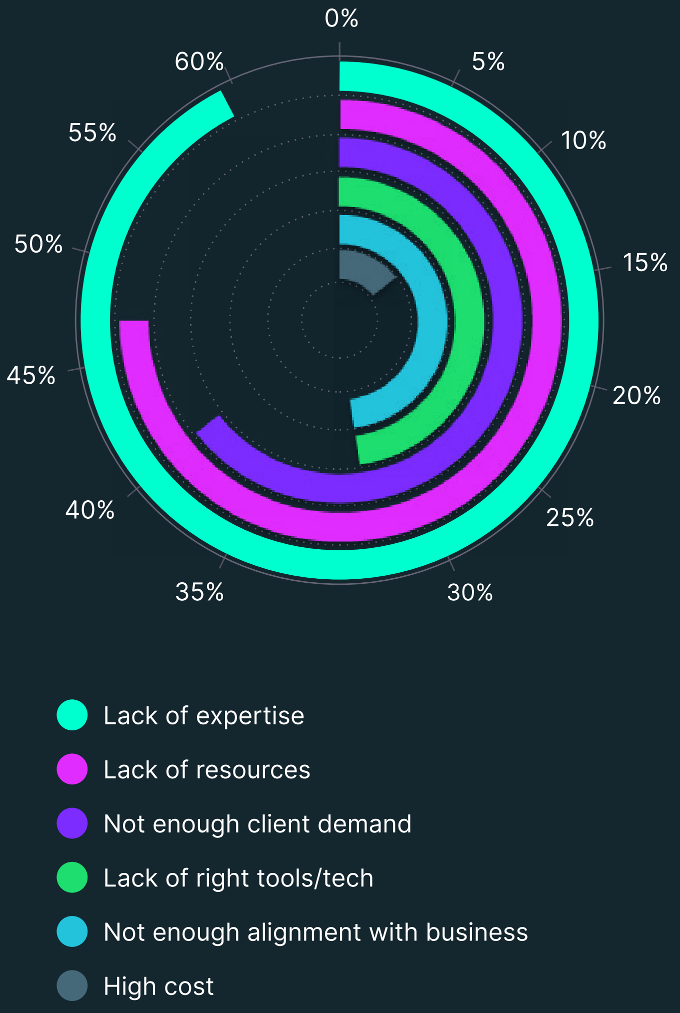
Why Some Providers Don't Offer Compliance Services

Of those not offering compliance services, nearly 60% say they lack the necessary expertise **(Figure 15)**. Almost half cite a lack of resources as a reason for not having a compliance offering.

Client demand is a higher concern for this segment than it is for those who provide compliance services, with 41% identifying it as a reason why they're not providing compliance services.

Lack of the right tools/tech and a lack of business alignment were each reported by 32% of providers, and high cost was a roadblock for 9%.

Key reasons providers aren't offering compliance services (fig 15)



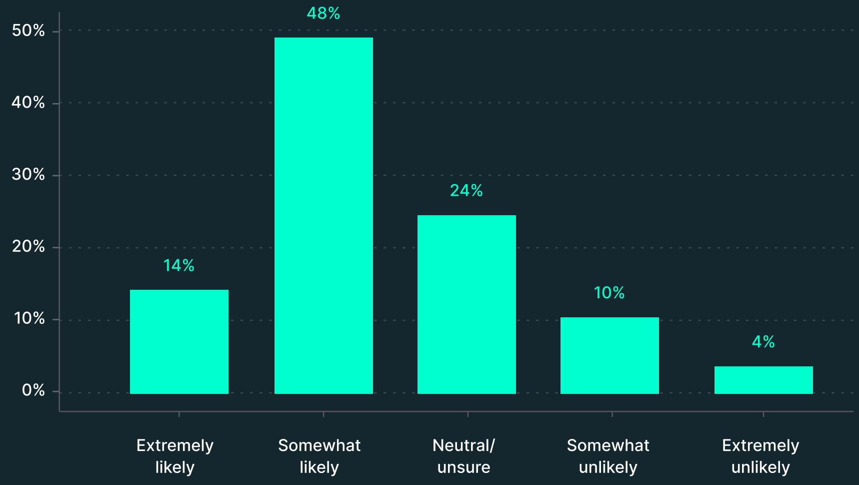
Most Providers Are Moving Toward Compliance

More than 3 in 5 providers not currently offering compliance services say they will likely offer them in the future **(Figure 16)**. Only 14% say it's unlikely.

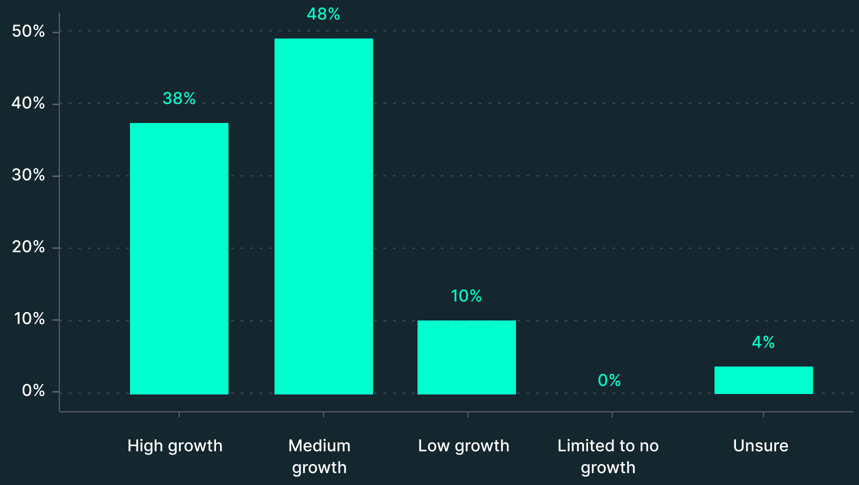
With 92% of all providers either currently offering compliance or likely to do so in the future, those with no plans to include the service could potentially be at a growth disadvantage.

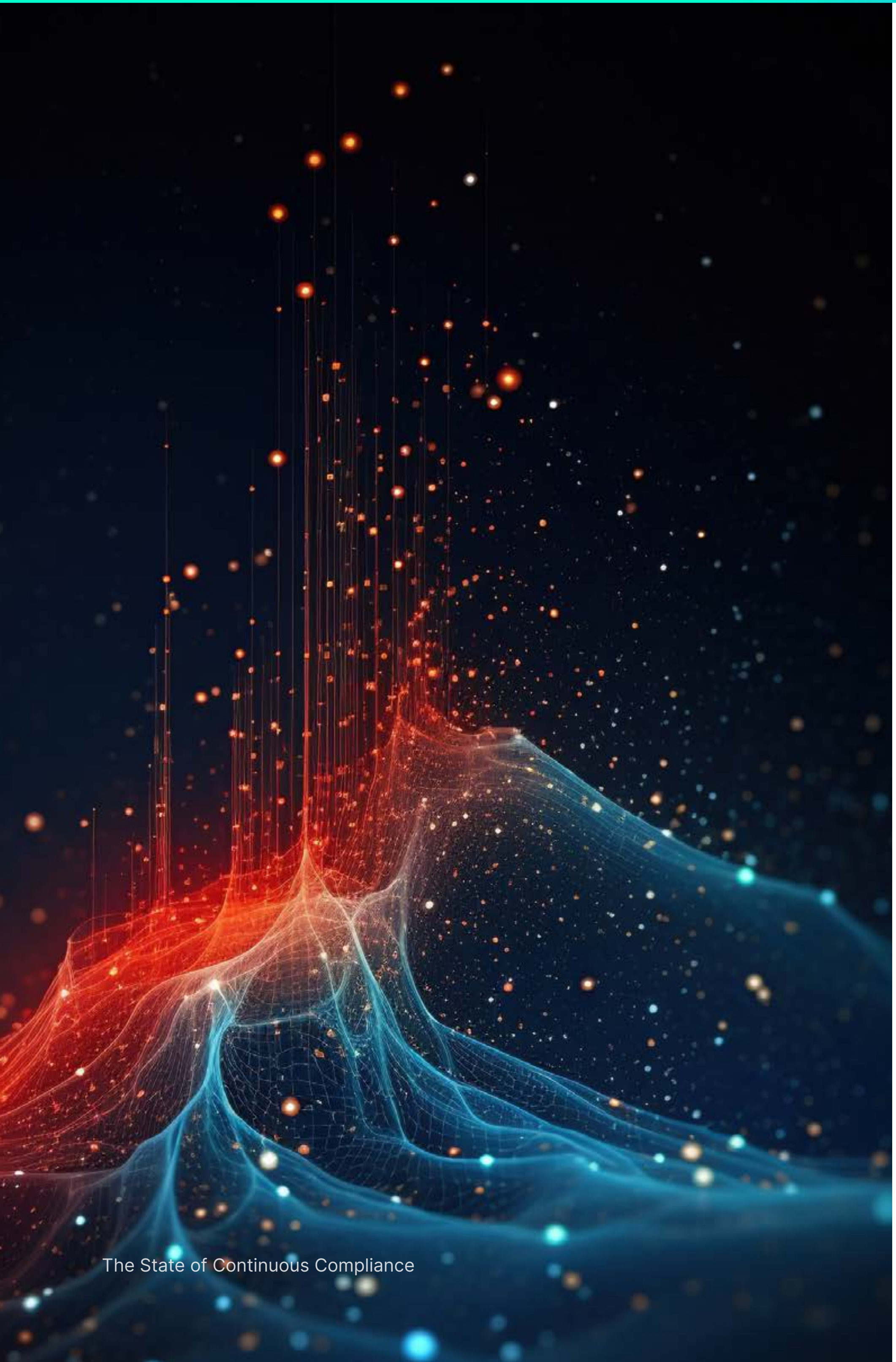
Among all providers, nearly three quarters view compliance as an area with high business growth potential **(Figure 17)**. That includes 38% of providers who aren't currently offering compliance services. Only 10% of this segment think compliance has low growth potential.

Likelihood of adding compliance services if not already (fig 16)



Compliance business growth potential among providers not currently offering these services (fig 17)





The Tools & Technologies Driving Compliance

The manual nature of traditional compliance work requires specialized knowledge and is often resource intensive. The many requirements and controls organizations must follow can be a lot to manage, especially when information is distributed across spreadsheets and folders.

While compliance automation platforms and GRC software have provided a boost for providers, many are missing the right tools to ease the burden. That's according to 36% of providers that report a lack of appropriate technology as a key challenge in maintaining compliance **(Figure 12)**—or a reason why they aren't offering any compliance services at all **(Figure 15)**.

Compliance Tools Explained

- **Spreadsheets** have long been the standard by which providers have managed cybersecurity compliance for their clients. This approach is often disorganized and can impact efficiency, productivity, and revenue potential. It can also put audits at risk if the information is hard to find or improperly documented.

- **GRC software** is a specialized technology designed to streamline and enhance the complex processes of governance, risk management, and compliance. It can consolidate various GRC activities into a single tool, reducing time and resources required.

- **Compliance automation platforms** enable providers to build and manage end-to-end cybersecurity and compliance programs at scale, helping continuously monitor security posture and compliance status as obligations change.

- **Homegrown solutions** provide a DIY approach for providers that want a tool custom-built for their business needs. However, this requires additional time, resources, expertise, maintenance, and costs, which many organizations can't spare.

> “
>
> The right compliance tool creates a broader, differentiated offering with higher value for customers, which means more MRR and ARR. Customers get stickier, churn goes down, and your net retention goes up because you're selling them more things to help maintain compliance or improve their security postures.
>
> Ultimately, your margins should get better if you're using the right tools and technologies and have the right partners.
>
> **Rahul Bakshi**
> Chief Product Officer, Apptega

Half of Providers Are Still Using Spreadsheets

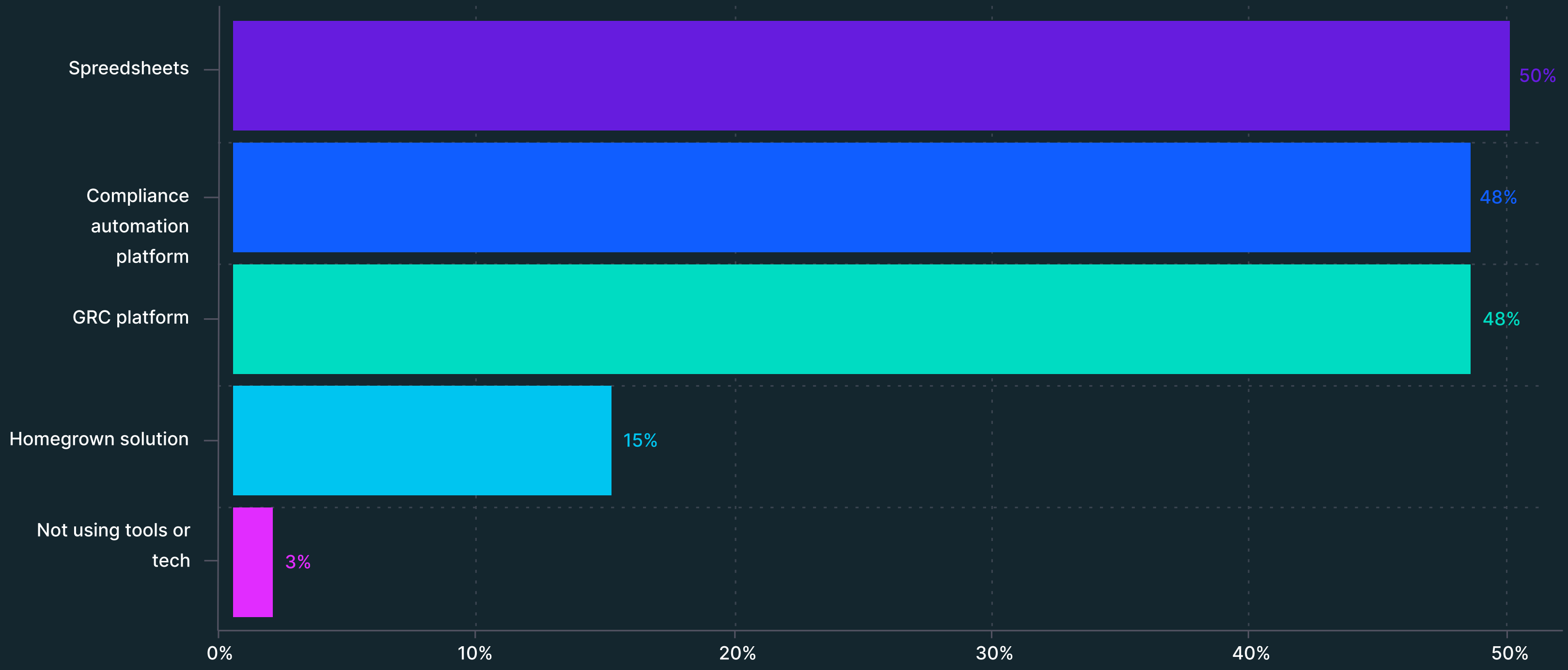
Of the providers offering compliance services, half are still using spreadsheets to track, measure, and report on cybersecurity compliance for their clients **(Figure 18)**. And some providers aren't using any tools at all.

While compliance automation and GRC platforms are each used by 48% of providers (a combined 80% of the total), these technologies are used in conjunction with spreadsheets nearly half of the time.

Though 87% are open to delivering their services through a compliance automation platform (Figure 7), only about half of these providers are currently doing so.

With so many providers using spreadsheets and a **disproportionally small percentage using compliance automation platforms compared to overall interest**, forward-thinking providers can capitalize on the opportunity to differentiate through technology.

Percentage of providers using various tools and technologies (fig 18)



Automation May Improve Growth and Efficiency

Percentage difference between providers using automation at least most of the time vs. sometimes/ never.

1. They have higher ARR/MRR growth goals

24% of providers using automation at least most of the time have target growth of more than 50% versus 15% of those who sometimes or never use automation **(a 46% difference)**.

46%

2. They're more confident in meeting their revenue goals

78% feel they are likely to hit their goals vs. 53% **(a 38% difference)**.

38%

3. Their risk assessments take less time

32% say assessments take hours or days vs. 8% (**a 120% difference)**.

120%

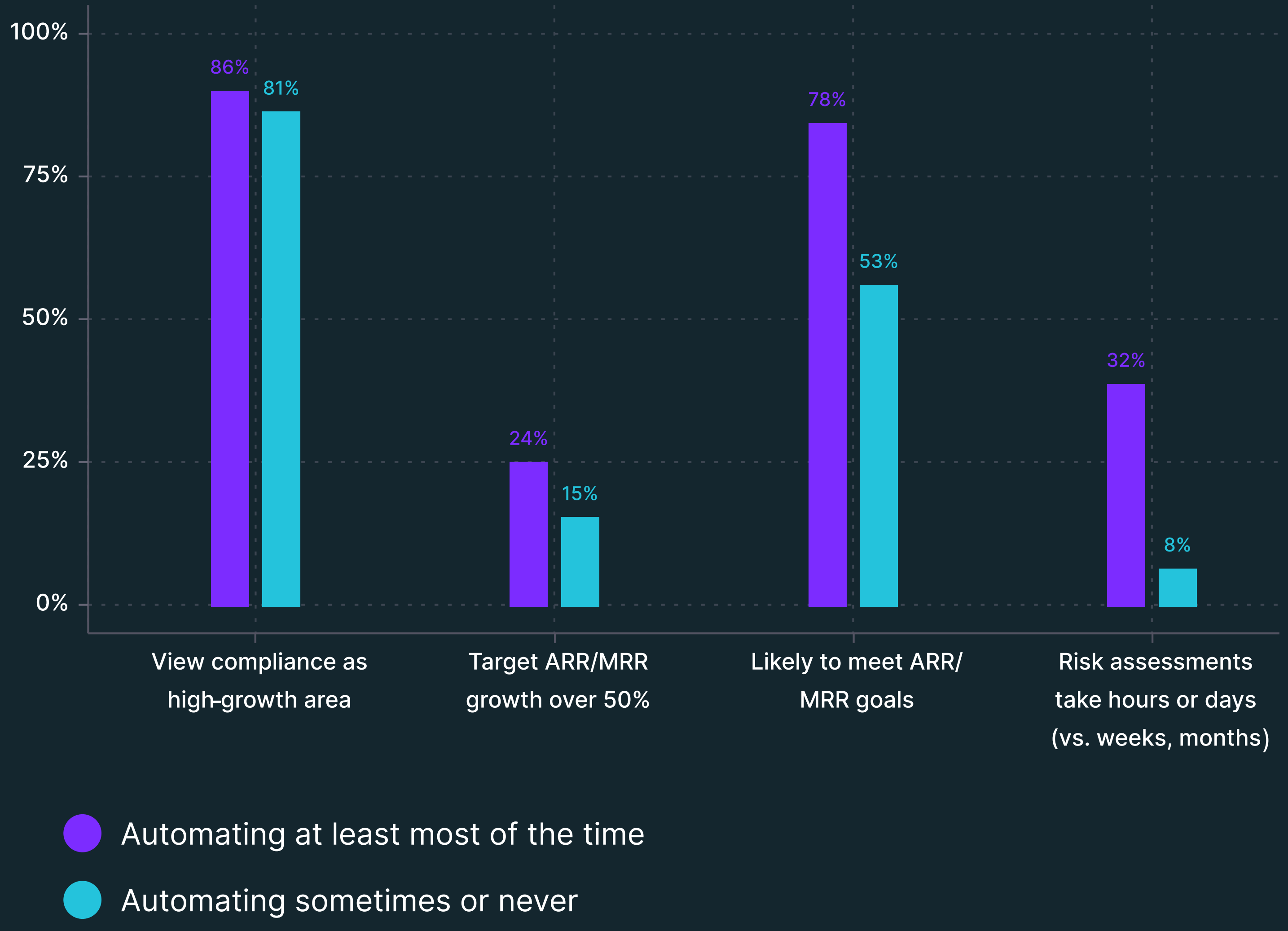
4. They're more confident in their ability to scale

95% are confident in their ability to immediately scale compliance services for additional customers versus 68% **(a 33% difference)**.

33%

Overall, providers using automation at least most of the time have more positive compliance outlooks than those who aren't **(Figure 19)**:

Goals and outcomes by automation level (fig 19)



How Apptega Partners Compare

Today, more than 20,000 security and compliance programs run on Apptega globally, many of which are delivered through our expanding provider ecosystem.

On average, these partners experience a 400% return on their investment in year one by using Apptega as the compliance “wrapper” to bundle, validate, and show the value of their cybersecurity services. In an increasingly commoditized market, our partners are delivering continuous security and compliance offerings that set them apart from the competition and maximize growth opportunities.

In this section, we examine how Apptega customers compare to the non-partners within this report.

Apptega Partners Have More Optimistic Goals and Outcomes

1. More of their revenue comes from compliance

21% get more than half of their revenue from compliance versus 13% of non-partners.

2. More of their compliance revenue is recurring

36% get more than half of their compliance revenue from recurring engagements versus 26% of non-partners.

3. They have higher ARR/MRR goals

62% have double-digit ARR/MRR growth goals versus 56% of non-partners.

4. They're more confident in meeting their ARR/MRR goals

67% say they are likely to hit their goals versus 43% of non-partners.

5. They're more likely to view compliance as a high-growth area

82% agree that compliance has high growth potential versus 60% of non-partners.

6. They see more value in continuous compliance

90% are interested in turning one-off compliance projects into continuous engagements versus 60% of non-partners.

7. Their clients are more interested in compliance

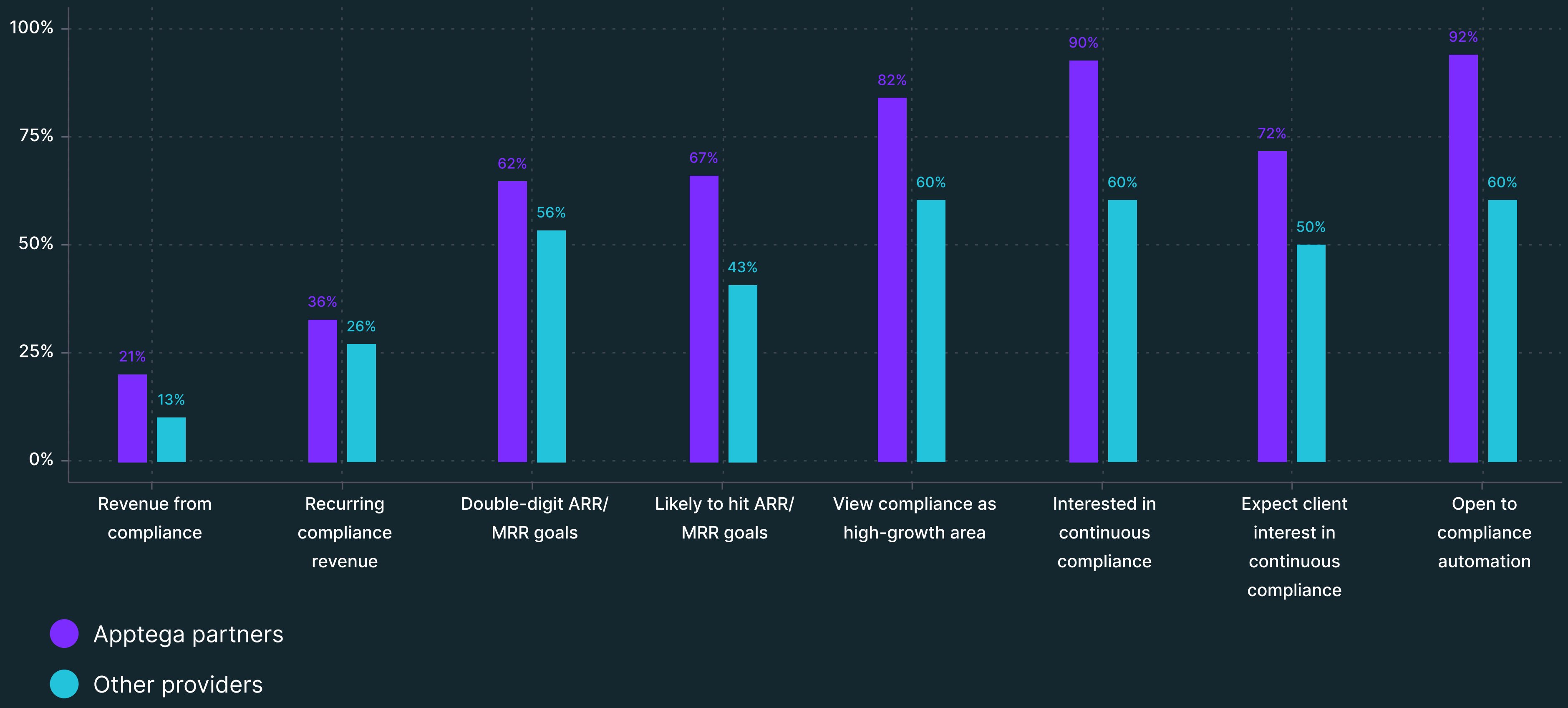
72% say clients would be interested in continuous compliance versus 50% of non-partners.

8. They're more open to compliance automation

92% are open to using a continuous compliance solution to automate workflows and gain real-time visibility into compliance status vs. 60% of non-partners.

Compared to other providers, Apptega partners have higher revenue from compliance, more recurring revenue, more ambitious ARR/MRR goals, and generally see more value in continuous compliance as a service for their clients **(Figure 20)**.

Compliance outlook: Apptega partners vs. non-partners (fig 20)



Summary and Next Steps

With benchmarking data that doesn’t exist anywhere else today, this inaugural State of Continuous Compliance Report aims to help providers realize new business opportunities and go to market more effectively with lucrative security and compliance solutions.

According to the findings, compliance is viewed as a high-growth area for managed service and security providers with aggressive growth and revenue goals. However, it currently represents a disproportionally small percentage of overall business and revenue, despite the complex regulatory and risk landscape their clients face.

Most providers face significant challenges maintaining compliance for their clients, including a lack of expertise, resources, and capable tooling. So, while the vast majority of providers are interested in improving recurring revenue through continuous compliance as a service offerings, few are capitalizing on the opportunity.

Overcoming these challenges presents tremendous upside, as those offering managed compliance as a service and employing automation tools were more optimistic about revenue growth, efficiency, and outcomes.

Recommended Next Steps for Providers

1. Package your services as aformal compliance offering

Doing so can help you capitalize on services you're likely already offering. In particular, bundling the entire end-to-end compliance program and managing it through a technology platform can deliver greater value, recurring revenue, and customer stickiness.

2. Differentiate your compliance services

Go beyond strictly consultative offerings and typical risk assessments that limit recurring revenue. Offering compliance as a managed service can help you fill a gap, improve revenue, and stand out from the competition.

3. Broaden your framework-based services

If you're not already offering framework services, doing so can uncover new and expanding opportunities. To further differentiate these services, consider framework crosswalking to meet a growing need to manage multiple frameworks. And don't ignore less-offered—but still important—frameworks such as ISO 42001.

4. Consider continuous compliance as a service

Turning one-off projects into long-term client relationships can help you increase recurring revenue, expand margins, and improve customer retention. Despite massive interest, few providers are taking this approach, which provides a massive opportunity to differentiate.

5. Ditch the spreadsheets

Adopting the appropriate technology—such as GRC software or a compliance automation platform—can help you create a broader, differentiated, and more valuable offering for your clients. Automating compliance can be especially beneficial in terms of revenue growth and efficiency.

6. Work with a technology partner.

The right partner can provide the technical and go-to-market support you need to acquire, grow, and retain clients, helping you maximize capacity and recurring revenue.

Overview of Methodology and Demographics

This 2024 State of Continuous Compliance Report is based on a survey of 115 managed service providers that offer security services.

The survey was confidential and didn't capture company-specific information or other data that could risk provider privacy or increase bias beyond what is inherent in the sampling frame or makeup of the survey.

The results of the survey and findings within this report are not intended to be conclusive. Instead, they provide a snapshot of how providers deliver compliance today and suggest potential opportunities for advancement.

By providing benchmarking data that doesn't exist anywhere else today, the report aims to help providers realize new business opportunities and go to market more effectively with lucrative security and compliance solutions.

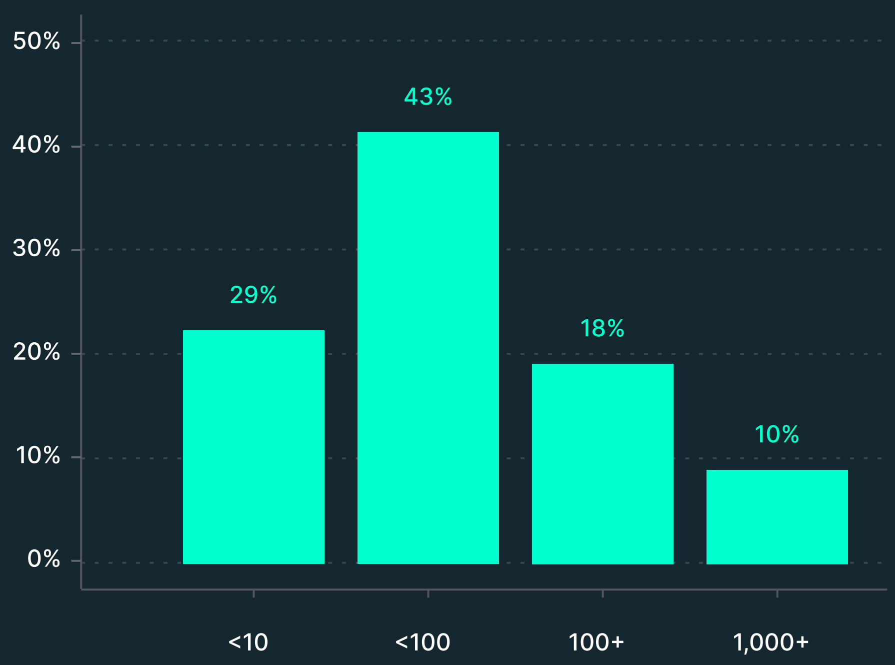
Provider Types

44%	**32%**	**19%**	**15%**	**7%**	**11%**
MSP	MSSP	MDR	XDR	Primarily Consultants	Other

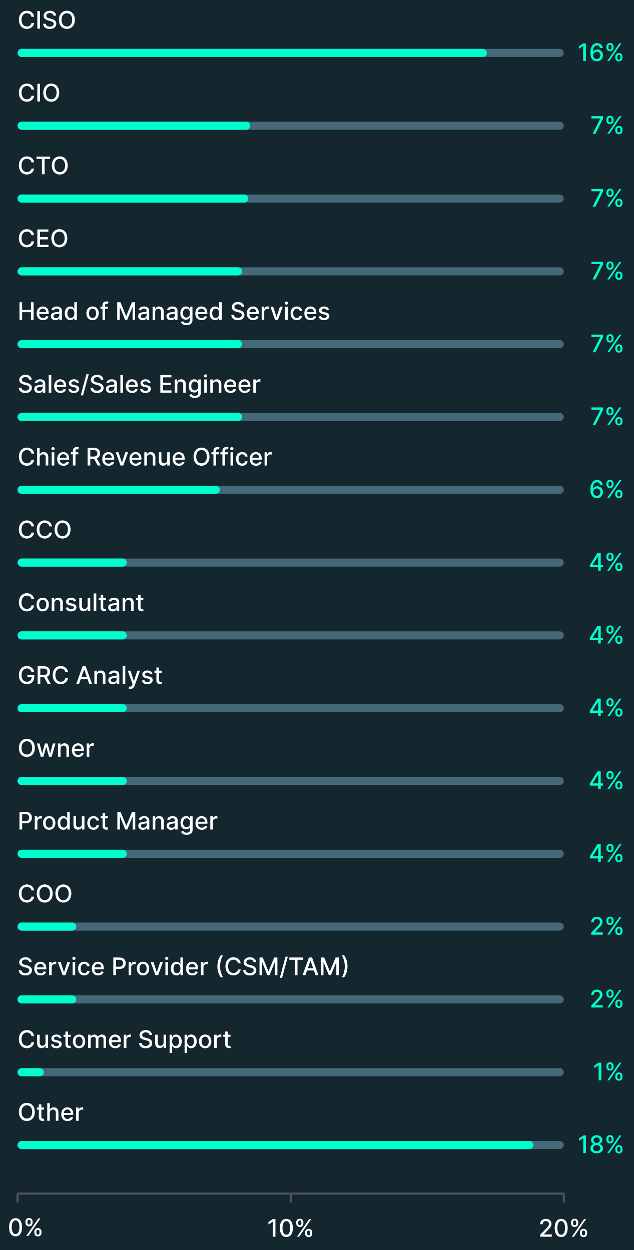
Location

90% in the United States

Company Size



Business Role



Apptega

About Apptega

A perennial G2 leader across various risk management categories, Apptega is the end-to-end cybersecurity compliance platform that security-focused IT providers and in-house teams use to build and manage cybersecurity compliance programs simply, quickly, and affordably. It’s trusted by hundreds of MSSPs, MDR companies, and security-focused MSPs that are growing lucrative compliance practices, creating stickier customer relationships, and winning more business from competitors.

Visit Apptega.com to learn more