FORRESTER®

The Partner Opportunity For Microsoft Security Partners

A Total Economic Impact™ Partner Opportunity Analysis

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY MICROSOFT, NOVEMBER 2025

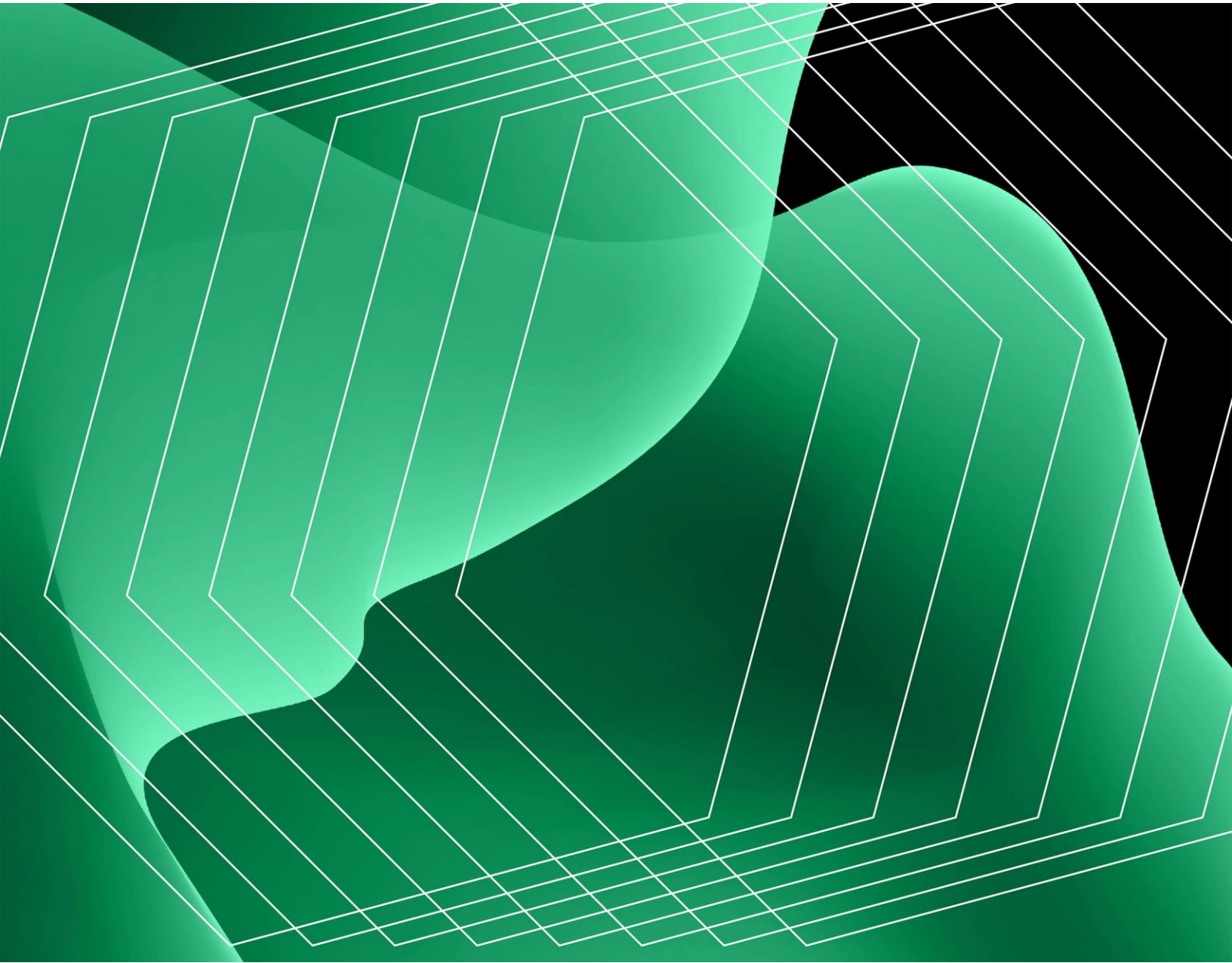


Table Of Contents

Consulting Team:

Luca Son

Cassandra Halloran

Jonathan Lipsitz

ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

Introduction

The security landscape and partner opportunities to deliver services around Microsoft's security and compliance solutions were transformed in fiscal year (FY) 2025 and the first quarter of FY 2026 because of the rapidly increasing interest in and adoption of AI in the workplace. AI, the ongoing customer desire for cost reduction through vendor consolidation, and Microsoft's continued investment in creating a unified security platform comprising best-of-breed solutions all contributed to a 20% increase in the partner expected-revenue opportunity at an enterprise customer. Microsoft partners that invested in their internal capabilities, especially those related to data security in the era of genAI, saw significant growth in over the past 15 months due to new market opportunities and expect this trend to continue throughout FY 2026 and beyond.

The past 15 months have seen a fundamental change in the role of IT security in terms of imperative, focus, and approach. The rapid rise of genAI is a main driver of this shift. While businesses and IT professionals have always needed good security and compliance solutions, it was very often a reactive, check-the-box activity to have good-enough security, be compliant, and/or qualify for cyber insurance. One result of this was constant and chronic underinvestment. Because of genAI, the underinvestment bill has come due. IT organizations that were previously short on time also need to support an entirely new solution area. Data security, compliance risks, and governance concerns have grown significantly. All other areas of IT security, such as identity, data, and endpoint protection, also need to be improved as part of becoming a high-performing and secure AI-enabled company.

This has profound implications for security and compliance service providers. Data Security and Compliance has become the main driver of partner opportunities and brings all other security disciplines along with it. Services and technology-based offerings need to be more agile and proactive, and they need to bring together signals from multiple areas to protect against more complex attacks, including the use of AI by bad actors. Advisory services are in high demand to help customers become AI-ready. Longer-term managed services opportunities are expanding to include all aspects of security and compliance in support of AI.

On top of all of this, customers are still demanding cost and internal effort reductions. In part, this can be achieved through vendor/product consolidation. IT service providers are also harnessing the power of AI to reduce their own efforts, especially in managed services like managed security operations center (SOC) and/or managed extended detection and response

(XDR). Today is a time of dramatic change for IT security: The threats are more complex and evolving rapidly; customers' needs are greater; and IT service providers have new AI-powered tools, such as Security Copilot, to help customers become more secure at a lower cost.

In order to understand the impact of these trends on the partner ecosystem, Microsoft commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential business opportunity partners may realize by building and scaling Microsoft Security practices.[1] "Microsoft Security" is a broad term that encompasses all products and services across six product families: Microsoft Defender, Microsoft Sentinel, Microsoft Entra, Microsoft Intune, Microsoft Security Copilot, and Microsoft Purview.

In this study, Forrester uses the term "security" as shorthand for one or more of the following solution areas built around the seven product families:

- **Microsoft 365 Security.** This solution area covers activating and managing everything security-related in Microsoft 365, including SOC/security information and event management (SIEM) specific to telemetry coming from the security and compliance features within Microsoft 365 E5.
- **Multicloud Security.** This solution area includes securing Azure and other public clouds' infrastructure, apps, and data.
- **Data Security and Compliance.** These solutions include data security (information protection, data loss prevention, and insider risk management) eDiscovery, governance, and privacy.
- **Identity.** Identity and access management (IAM) provides core digital identities to knowledge and frontline workers as well as to third parties. This solution area includes Microsoft Entra ID, Zero Trust network access, and capabilities like single sign-on (SSO) and multifactor authentication (MFA).
- **XDR.** Extended detection and response is primarily a proactive managed services opportunity and a natural extension of endpoint detection and response. XDR includes endpoints, identities, data, and applications both on-premises and in the cloud. XDR is an expansion of the Microsoft 365 E5-specific SOC/SIEM opportunity described above.

Expected revenue opportunity (with attach rates applied)

$54.35 per user per month

Expected revenue year-on-year growth

20%

Partner estimates are based on a new enterprise customer (5,000 knowledge workers) and a 36-month customer journey

This year's study focuses on what has changed for security partners in FY 2025 and the first quarter of FY 2026, as well as the outlook for the remainder of FY 2026. This includes 1) what customers want from Microsoft partners, 2) how Security partners make money, and 3) the best practices and investments that create success.

To better understand the revenue streams, investments, and risks associated with a Microsoft security practice, Forrester interviewed representatives from 15 global and regional partners with practices in one or more of the aforementioned solution areas. These interviews build on more than 80 interviews with Microsoft partners that were conducted in previous years as well as with dozens of organizations that buy partners' services.

Forrester created a partner opportunity model for enterprise customers based on what leading partners achieved in FY 2025 and Q1 FY 2026. This model quantifies the opportunities for deployment, advisory services, solutions development (e.g., repeatable IP, custom solutions, and advanced integration work), and managed services. Accounting for attach rates, Forrester found that the expected-revenue opportunity for a new enterprise customer is up by 16% year over year.[2]

Forrester also conducted a deep-dive analysis of cloud solution provider (CSP) partners' security opportunities.[3] It provides additional guidance to CSPs on how Microsoft's messaging resonates with customers; how partners are leveraging incentive programs; revenue opportunities and typical land-and-expand scenarios with small, medium, and corporate (SMC) customers; and which Microsoft solutions and partner services are particularly well positioned for SMC customers.[4]

Another Forrester study examined how Microsoft 365 Copilot and agentic AI are growing the Modern Work revenue opportunities.[5] Forrester recommends that partners with a Modern Work practice refer to that study as well.[6]

“[We estimate that] 60% to 70% of our incidents are handled automatically. … We think we can triple our revenue without hiring new personnel. … AI is enabling us to do more with less.”

HEAD OF SECURITY SERVICES, SYSTEMS INTEGRATOR

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews with partners of various sizes from around the globe, Forrester constructed a Total Economic Impact™ framework for those partners considering building and growing one or more security practices.

The objective of the framework is to identify the revenue streams, investments, and best practices that affect the investment decision. Forrester took a multistep approach to evaluate the holistic opportunity for partners building and growing a Microsoft security practice.

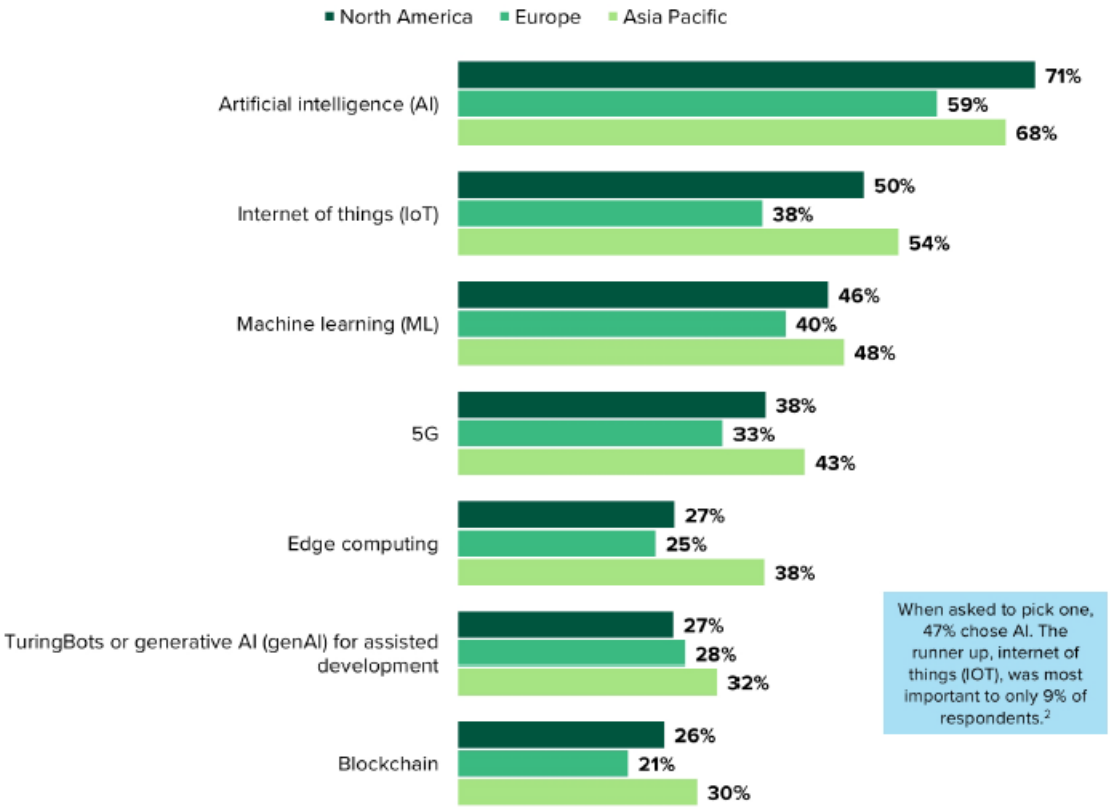
1. **Due Diligence**
   Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Microsoft 365 Security, Data Security and Compliance, and Identity.
2. **Interviews**
   Interviewed representatives at 15 partner organizations with one or more existing Microsoft 365 Security, Multicloud Security, Data Security and Compliance, Identity, or XDR practices to obtain data about revenue streams, investments, and best practices.
3. **Composite Organization**
   Designed a composite organization based on characteristics of the interviewees' organizations.
4. **Financial Model Framework**
   Constructed a financial model representative of the interviews using the TEI methodology. The model normalizes all results as a per-user per-month opportunity at an enterprise customer with 5,000 knowledge workers on a 36-month customer journey.
5. **Case Study**
   Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Market Trends

THE CUSTOMER PERSPECTIVE

This section incorporates Forrester's research and survey data to understand what is driving customers' demand in terms of their priorities and the services they are looking for. "The State Of Technology Services, 2025, Part 1: Co-Innovation Services" Forrester report revealed that AI is, by far, the top emerging technology for which organizations are planning to use third-party services over the next 12 months.[7]

"For which of the following emerging technologies do you expect your organization to use third-party service providers in the next 12 months?"



Note: Not all response options are shown
Source: Forrester's Business And Technology Services Survey, 2024

Forrester's Priorities Survey, 2025, which polled 5,449 business and technology professionals, found that "enhance IT security" is the third most important IT priority over the next 12 months, slightly behind improving the customer experience and the employee experience — and ahead of 14 other investment categories.[8] For security decision-makers, using the "built-in security capabilities from Microsoft, Google, AWS, or other tools instead of standalone security technologies for the same capability" was the second-highest IT security priority over the next 12 months.[9]

IT Security Priorities (Top Five)	
Improve application security and/or product security capabilities and services	31%
Use built-in security capabilities from Microsoft, Google, AWS, or other tools instead of standalone security technologies for the same capability	26%
Improve threat intelligence capabilities to proactively identify security threats targeted to our organization or industry	26%
Improve access management capabilities and policies for employees and partners	24%
Improve device security and services to support the capabilities for employees to work from anywhere they choose	23%

Base: 5,449 business and technology professionals
Source: Forrester's Priorities Survey, 2025

Data Security and Compliance is a growing priority for IT professionals. Forrester's Priorities Survey, 2025, showed that organizations' top planned activities are all opportunities for partners to help their customers. The top four priorities were "invest in/expand our use of governance, risk, can compliance technologies," "enhance our training and awareness efforts," "improve oversight with better risk data analytics," and "invest in/expand our use of information security technology solutions."[10]

Lastly, the move to public clouds and SaaS software continues to be a high priority for IT organizations. In Forrester's Industry- And Customer-Supporting Software Survey, 2025, which polled 2,478 software decision-makers, their largest concern when it comes to using SaaS is "data security and protection against cybercrime"; "compliance with data privacy laws" was in the middle of the list.[11]

THE PARTNER PERSPECTIVE

Partners shared their views on the high-level trends that are driving growth and what they believe will be even more important during the next year:

- **GenAI is creating more partner opportunities and the need to broaden internal capabilities.** All partners said that genAI has become the largest sales conversation topic and is increasing the number and size of deals. One partner estimated that in the next year, "AI should bump up revenue by 20% to 25% across all solution areas." Customers' increased focus on AI has increased their need for AI-readiness advisory services and for partners to improve their advisory capabilities for planning, change management, and training. Many partners also reported needing to broaden their capabilities beyond security to include areas like information management and low-code development.

> "AI adoption is driving a 30% to 35% increase in data security engagements. … Customers realize they need to overcome fear and build confidence before scaling AI."
>
> MANAGING DIRECTOR CYBERSECURITY, SYSTEMS INTEGRATOR

> "AI is a seismic shift in what we advise customers on. But we still go back to the basics of data security and identity. The 'what' has changed, but not the 'how.'"
>
> GLOBAL MICROSOFT SECURITY SERVICES LEAD, SYSTEMS INTEGRATOR

- **The integrated and best-of-breed Microsoft solution stack increases partners' opportunities.** Partners said that their customers increasingly view Microsoft's various security solutions as best of breed, not just an integrated solution stack. This is making it easier to get customers to adopt more Microsoft solutions and is also contributing to competitive takeouts in more areas. Consolidating onto Microsoft also makes it easier for partners to sell and deliver managed services. The genAI imperative is creating more E3 to E5 upsell opportunities, either with the Microsoft Defender or Purview Suites add-ons or with the full Microsoft 365 E5 SKU, which greatly increases partner opportunities.

> "Our growth in the security area is coming from Microsoft. Security has become proactive and intelligence-based, and this is where Microsoft has moved ahead of the competition. Microsoft can now meet all of our customers' security needs."
>
> COFOUNDER AND EXECUTIVE DIRECTOR, SYSTEMS INTEGRATOR

- **Customers increasingly focus on cost reduction.** Throughout the past 15 months, customers asked partners to help them reduce their IT security spend. This accelerated in the first half of calendar year 2025 and continued through the second half of the year, given increasing economic uncertainty and angst. Consolidating onto Microsoft's security stack is a way for customers to reduce costs because they are often paying twice for solutions that do the same thing; it also reduces internal efforts to manage multiple solutions. Partners reported more competitive takeouts than in previous years and across more solution areas, including identity, various Microsoft Defenders, and endpoint security/management.

  At the same time, customers are expecting partners to maximize the value of their existing Microsoft investment. Partners also reported seeing more competition with pure play vendors competing at a lower price points. To address this, partners are breaking projects into smaller chunks, discounting first-year deals, and introducing flat-fee and co-managed pricing models to win and retain customers.

> "We are seeing competitor takeouts across practice areas. This has been the case for [Microsoft] Entra for a while, and we are seeing increased interest in other areas."
>
> CHIEF COMMERCIAL OFFICER, SYSTEMS INTEGRATOR

- **More partners are moving into the SMB/SMC area.** Many partners that focus on enterprise customers are starting to sell to small and medium-size businesses (SMBs) and SMC customers. Partners said that smaller customers lack the internal skills to manage their security solutions and protect themselves against increasingly complex threats. The lack of resources and better deal economics from the customer's perspective create more managed services opportunities. To serve this customer segment cost effectively, partners are creating simplified solutions and applying more automation to service delivery, including Security Copilot and other in-house tools. One partner said that AI automation projects that include Security Copilot automated 80% of help desk tickets and has made the managed services team 40% more efficient.

> "SMC [small, medium, and corporate] is a high-growth area for us. Smaller companies lack the internal resources, especially in areas like SOC, which creates managed services opportunities."
>
> STRATEGIC CONSULTANT, SYSTEMS INTEGRATOR

- **Microsoft's partner programs and support are driving success.** Partners said that Microsoft's partner programs have improved over the past year in terms of methodologies, such as partner engagements, co-sell, co-marketing, go-to-market

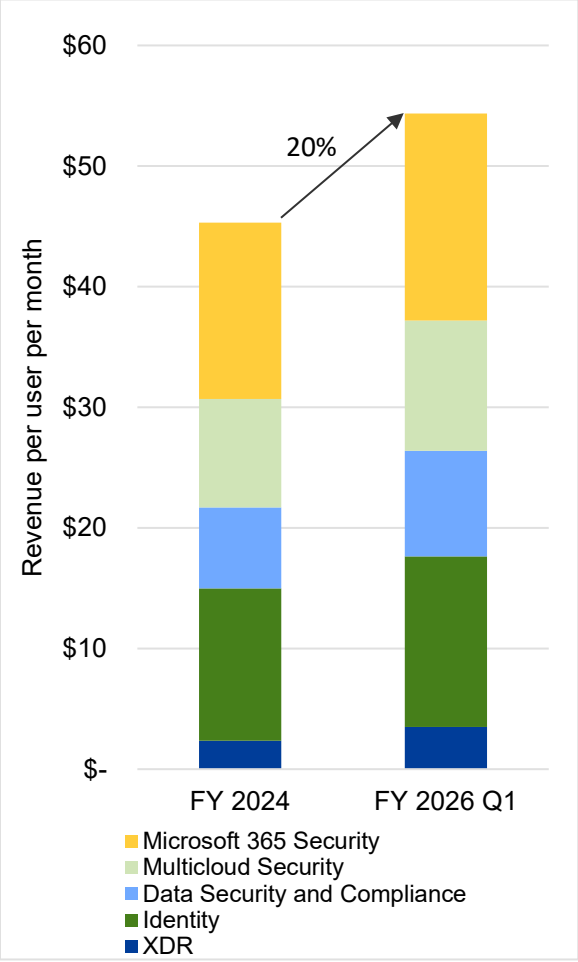
motions, processes, and funding incentive programs like Microsoft Commerce Incentives (MCI). (Partners shared with Forrester recommendations on how to improve support and programs, which were shared with Microsoft.) They said that a little bit of early funding can make a huge difference in creating large, multiyear delivery programs and win deals against pure play competitors. Partners are also investing more time in achieving the various Microsoft Security Specializations and getting into programs like the EA Security Accelerator (EASA), formerly Cybersecurity Investment Program (CSI), which is by invitation only.

> "Microsoft's programs and funding mechanisms have matured over the last year. They are instrumental for winning early engagements and future upsell opportunities."
>
> **DIRECTOR OF STRATEGIC ALLIANCES, SYSTEMS INTEGRATOR**

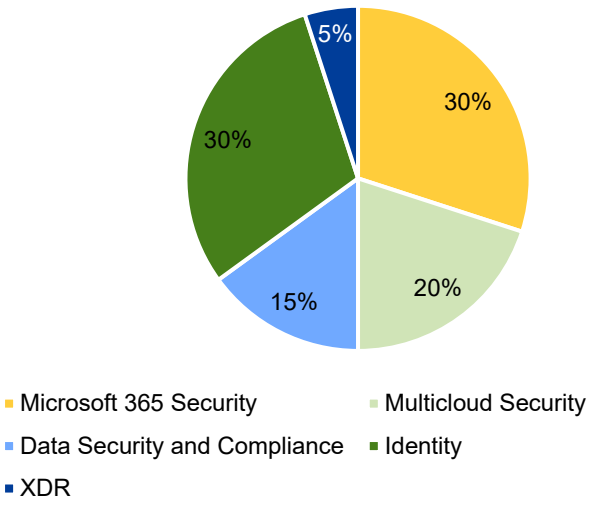
The Partner Opportunity

The trends discussed above resulted in increased revenues across all solution areas in FY 2025 and Q1 FY 2026, both in terms of total revenue potential (i.e., what partners are offering) and the expected revenue associated with the likely bundles of services and products that customers are buying (attach rates applied). The expected revenue opportunity grew by 20% for a partner on a three-year journey. The two largest year-over-year expected revenue growth opportunities in percentage terms were Data Security and Compliance and XDR. The genAI imperative has increased Data Security and Compliance's expected revenue by 31%. Partners saw a 49% increase in expected revenue for XDR as they mature their offerings, streamline their operations, and expand into the SMC market.

Year-Over-Year Growth (Expected Revenue)



Expected Revenue Opportunity Mix



Forrester also broke down the expected revenue opportunity across four service areas: deployment, advisory, solutions development, and managed services.

- **Deployment opportunities grew by 17%.** Deployment is the typical entry point for new customer engagements, competitive takeouts, and Microsoft 365 E3 to E5 migrations, either the full Microsoft 365 E5 SKU or the Microsoft Defender Suite or Purview Suite add-ons. Partners viewed deployments as a consistent way to create new business that also drives advisory services and can evolve into solutions development and managed services opportunities.
- **Advisory services grew by 35%.** Advisory services saw the largest increase, as customers demanded comprehensive Data Security and Compliance services as part of genAI readiness and adoption. Partners are seeing more advisory opportunities to prepare customers for increasingly complex threats driven by the use of AI by bad actors. Growing regulatory demands are also increasing demand for advisory services. Advisory services include upfront strategy and planning work as well as adoption and change management services. Advisory services help partners differentiate their services, improve the stickiness of their offerings, and increase security success.

- **Solutions development grew by 13%.** Solutions development encompasses repeatable intellectual property (IP) created by partners, either as standalone offerings for sale or to enhance the efficiency of deployments and managed services. It also includes custom solution development and advanced integration work. Resalable IP focused on improving manageability, signal ingestion, monitoring, and alerting. Data Security and Compliance partners contributed custom IP, such as compliance connectors. Notably, partners are now prioritizing new offerings in data security, including solutions aligned with responsible AI practices.
- **Managed services grew by 24%.** Managed services are critical for helping partners scale and build predictable, recurring revenue streams. They offer greater upsell opportunities, provide potentially higher margins, and support repeatable business models. Partners emphasized two key themes: 1) leading with go-to-market messaging that highlights proactive services to help clients stay ahead of an increasingly complex threat landscape and 2) driving operational efficiency by ingesting more signals across the Microsoft security stack, including solutions like Microsoft Sentinel and Microsoft Defender. Partners are also exploring how Microsoft Security Copilot can enhance analyst productivity and streamline operations, with some already reporting significant efficiency gains.

Revenue Opportunity By Partner Service

Partner service	Total revenue per user per month	Blended attach rate	Expected revenue per user per month	Expected year-over-year growth
Deployment	$19.90	61%	$12.15	17%
Advisory	$8.00	58%	$4.65	35%
Solutions development	$41.75	34%	$14.20	13%
Managed services	$59.40	39%	$23.35	24%
Total	**$129.05**	**42%**	**$54.35**	**20%**

Revenue Opportunity By Solution Area				
Solution area	**Total revenue per user per month**	**Blended attach rate**	**Expected revenue per user per month**	**Expected year-over-year growth**
Microsoft 365 Security	$46.15	37%	$17.15	17%
Multicloud Security	$25.00	43%	$10.80	20%
Data Security and Compliance	$22.05	40%	$8.75	31%
Identity	$22.90	62%	$14.15	12%
XDR	$12.95	27%	$3.50	49%
Total	**$129.05**	**42%**	**$54.35**	**20%**

MICROSOFT 365 SECURITY

Microsoft 365 Security involves activating and managing Microsoft 365 solutions securely. Partners are reporting more competitive takeouts and sunsetting outdated systems, particularly in the areas of Microsoft Defender and endpoint management. This highlights the emerging view that many of Microsoft's security solutions are best of breed, not just a unified security platform. Consolidation simplifies management for partners, increases partner revenues, and improves customers' security.

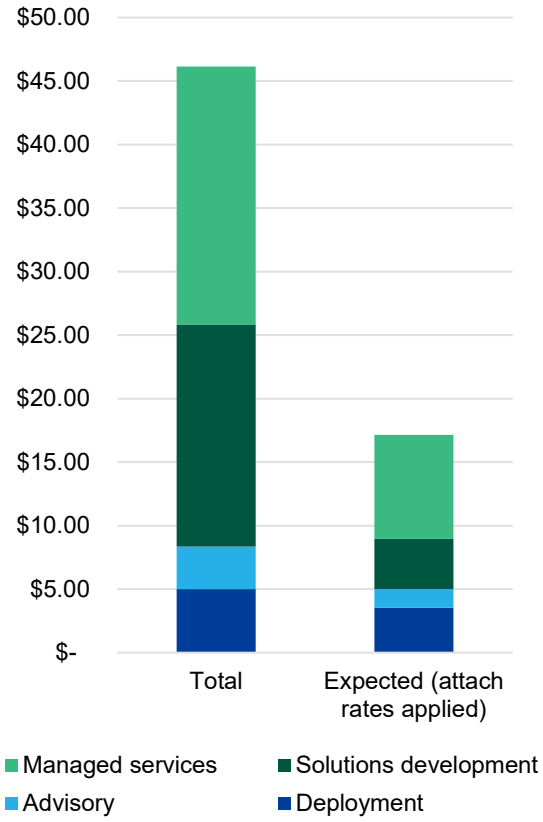
The combination of Microsoft 365 E5 and Microsoft Sentinel leverages native integration capabilities, lowering the total cost of ownership for clients and driving win rates for partners. This integration enhances a customer's security posture while optimizing costs. Threat protection remains a critical growth engine for partners. The robust capabilities of Microsoft Defender for Endpoint, Office 365, and Microsoft Sentinel are driving the greater adoption and expansion of security services. One partner reported growth of 50% from threat detection, endpoint protection, and email security.

- **E3 to E5 migrations and Microsoft Sentinel SOC/SIEM deployments drove an increase in deployment services.** Partners have seen a 5% increase in E3 to E5 migrations since FY 2024 as more customer organizations mature and see the value of E5 as part of AI readiness. SOC and SIEM deployments increased by 20%, showcasing more appetite to use Microsoft Sentinel.

- **Advisory services are becoming more important because of AI.** Partners emphasized that the upfront strategy and planning provided by their subject matter experts (SMEs) is crucial for setting organizations up for success and maximizing their subsequent investments in solutions development and managed services. The increasing complexity of threats, the expansion of the Microsoft 365 Security portfolio, and the need to secure Microsoft 365 Copilot are driving significant advisory opportunities.
- **Custom solutions help partners deliver their services and create new revenue opportunities.** Solutions development includes the resalable IP that partners create, which complements what Microsoft has built. This IP is often related to improved manageability, signal ingestion, monitoring, and alerting. Separately, one partner expected to expand revenue by selling services to help other Microsoft partners build their own solutions.
- **Managed services offer the largest opportunity in terms of revenue.** Forty percent of projects lead to managed services opportunities. The growth in opportunities with Microsoft Sentinel has allowed partners to grow their managed services offerings, enabling comprehensive end-to-end security operations and managed services. Partners offer a range of service levels, including 24/7 fully outsourced support. This growth underscores the increasing demand for advanced security monitoring and response solutions.

> “Microsoft Sentinel has come out of nowhere, and it was the horse at the back that’s now starting to lead the pack.”
>
> EXECUTIVE DIRECTOR OF PRODUCT, SYSTEMS INTEGRATOR

Microsoft 365 Security Opportunity



> “Security as a whole is the biggest growing rate that we have. It is about 30% overall year on year. We focus very, very heavily on security, and it is by far the largest delivery arm within our company right now.”
>
> DIRECTOR OF SECURITY, SYSTEMS INTEGRATOR

MULTICLOUD SECURITY

Cloud migration and consolidation have become pivotal strategies for customers and partners to manage complexity, phase out outdated or redundant systems, and reduce the burden of maintaining legacy infrastructure. This approach is significantly increasing opportunities in Multicloud Security as clients seek partners' help in navigating the complexities of hybrid and multicloud environments. This demonstrates the critical role of partners in providing comprehensive security solutions.

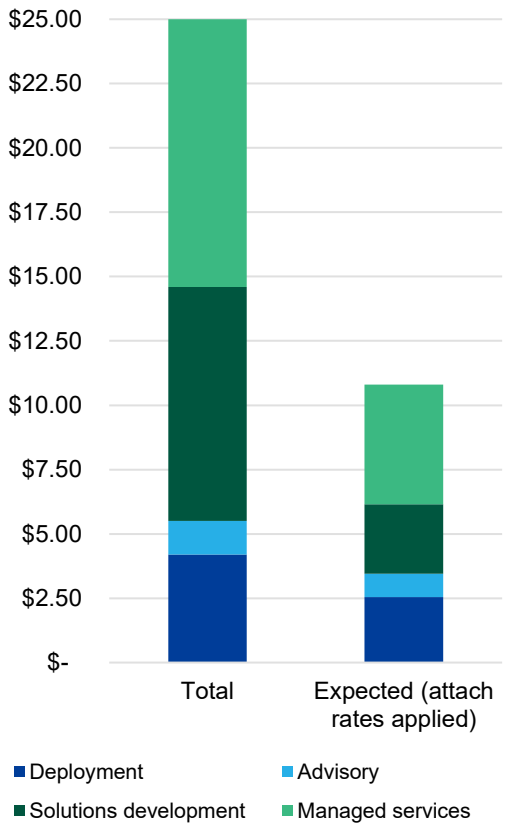
Partners told us of notable growth in Azure and cloud network security opportunities. One partner reported year-over-year growth of up to 45% with Azure depending on the geography, with service margins of up to 20%. One partner said: "We are increasingly discussing AI and large language models (LLMs). For example, the new cloud security posture management (CSPM) capabilities within Microsoft Defender for Cloud allow AI to analyze SaaS services and other organizational resources, creating a risk profile and enhancing [the] security posture across the entire landscape." This signals opportunities for partners to further build out their services. Partners reported success with deploying, configuring, and offering managed services with Microsoft Defender for Cloud Apps. They are also enhancing their security capabilities by increasing ingestion points and integrating third-party signals across hybrid and multicloud environments using Microsoft Sentinel and Microsoft Defender for Cloud. This integration enables comprehensive monitoring and threat detection, further indicating the importance of advanced security measures in today's digital landscape.

- **Expected revenue for deployment grew 13%.** Although deployment projects for Azure, Defender for Cloud, and similar services often start with a proof of concept or security assessment, the bulk of revenue comes from deployment activities. Partners provide services like Azure server migration, application migration, and security work related to Azure migration and transformation. One partner said: "We've seen some wins from integrating logs. There has been more success with [Microsoft] Defender for Cloud Apps across deployment and configuration services. We then have managed services to ensure new updates get deployed." While most partners specialize in Azure deployments, many are also capable of assisting customers with other public cloud platforms.
- **Advisory work is attaching at a higher rate as customers increase their cloud footprint.** Partners offer Azure security strategy, planning, and upfront governance work to ensure a successful cloud migration. One partner that specializes in setting up cloud centers of excellence to help leverage native cloud security capabilities for workload

protection and CSPM told Forrester: “Clients think if they have Azure and firewall security, they don’t need anything else. That’s a mistake.” These advisory services establish the practices, workflows, and technologies needed to secure cloud environments effectively.

- **Partners continue to create their own IP to increase revenue potential and margins.** Complex migration work opens up opportunities for partners to offer custom solutions, such as one partner’s compliance connector IP and another partner’s IP for requirements gathering and monitoring. Custom IP helps increase revenue potential and margins.
- **Multicloud Security deals increasingly include managed services.** Managed services for Multicloud Security are attaching at higher rates than in previous years as partners continue to help customers operate securely in the cloud. One partner told Forrester: “Almost all clients are multicloud. Our first choice is to sell managed services. Around 75% of our multicloud deals lead to managed services.”

Multicloud Security Opportunity



“Cloud security should drive additional revenue, supported by a cohesive product strategy from Microsoft. [Microsoft] Defender for Cloud enhances visibility and provides unified control over [the] cloud security posture.”

CYBERSECURITY AND INNOVATION STRATEGY LEADER, SYSTEMS INTEGRATOR

DATA SECURITY AND COMPLIANCE

The rise of genAI, including copilots and agents, is the largest driver of partner activities and new and expanded revenue opportunities. Partners have underscored the critical need for robust data security, compliance, and governance frameworks before deploying AI solutions. This strategic focus has led to double-digit growth for many partners, with advisory services being the primary entry point for genAI services.

There has also been a notable surge in the adoption of Microsoft Purview, which provides a comprehensive suite of capabilities across data security (including information protection, data loss prevention, and insider risk management), data governance, and risk and compliance. This reflects the growing importance of comprehensive data management and protection strategies. In response to the rising demand for genAI-related offerings, partners are expanding their teams to ensure readiness for and expertise in this transformative technology. This support is crucial for meeting clients’ needs and leveraging the full potential of genAI.

Partners are now moving beyond initial advisory and readiness engagements for data security and compliance into building recurring service models. Many are introducing managed offerings, such as compliance monitoring, insider risk management, and ongoing policy enforcement, to capture long-term value. These services often follow project-based professional services, where conversion rates can reach 75% to 90% and are positioned as critical for sustaining governance and risk reduction in an AI-enabled environment.

In addition to genAI, the regulatory landscape in Europe and the evolution of security frameworks like NIST CSF 2.0 are driving growing demand for Data Security and Compliance services. Compliance-specific partners are introducing new services centered on responsible AI, predominantly advisory or consulting, and often with a fixed upfront price.

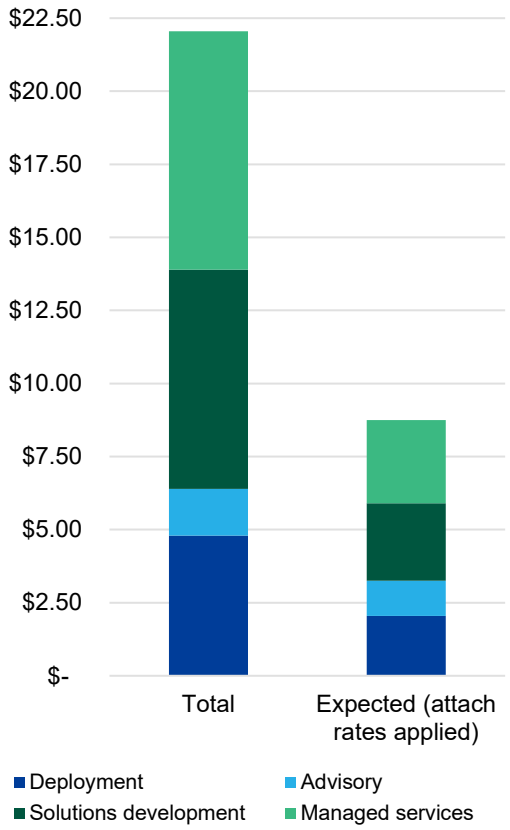
> "There has been a huge uptake in [Microsoft] Purview in the last six months. In the past, customers would say, 'Just turn [Microsoft] Copilot on.' … A year ago, we had two full-time people delivering [Microsoft] Purview, and now we have 20."
>
> CLOUD SECURITY PRACTICE LEAD, SYSTEMS INTEGRATOR

- **Expected revenue for deployment grew by 32%.** Partners have seen significant growth in the number of Data Security and Compliance projects over the past year. Joint go-to-market messaging, webinars, co-marketing, and partner engagements with Microsoft are leading to high win rates. Many partners provide services to get Microsoft 365 Copilot up and running as quickly and securely as possible. These projects include deployment, data services and remediation for initial users, as well as proactive controls and data classification. Other partners leveraged the increased demand in genAI to establish foundational security approaches for the AI era, such as Purview deployments: One partner launched Microsoft Purview projects through paid presales engagements, converting 80% to full implementation projects. These engagements also opened the door to additional offerings, such as data protection services.
- **The advisory services revenue opportunity grew the most and is attaching at 75%, the highest rate across offerings.** Advisory services for genAI readiness that include data and compliance projects are booming as customers prepare for genAI. One partner said: "Data security is a huge growth area. We have been working closely with Microsoft and utilizing [EASA's] data security component to help us capture these opportunities." One partner shared that its data readiness services typically cost around £400,000 and result in a 50% conversion rate, with half of the clients going on to purchase managed services.

- **Partners have developed, promoted, and actively monetized solutions that simplify Data Security and Compliance.** These offerings make compliance more manageable and efficient for customers, covering areas like information protection governance, e-discovery services, and compliance connectors. In parallel, partners are innovating in the data security space: One partner launched a responsible AI solution to "help with the customer journey from validation to adoption to all the controls in between." Another partner built proprietary IP "to manage Purview and compliance as a managed offering."
- **Security partners are offering more managed services for Data Security and Compliance.** Partners are creating and offering new managed services, such as compliance monitoring, insider risk management, and ongoing policy enforcement, to proactively address risk and expand one-time consulting and advisory engagements. The CEO of a managed services provider shared they are seeing "conversion rates in the 90s percent for follow-on technology work after an [around] $8,000 AI/compliance consulting engagement," signaling a strong appetite for continued data security and compliance services. The head of security services at a systems integrator said: "Data security is definitely increasing. Customers are willing to invest in this. We're attaching more managed services like insider risk monitoring to these services. … I think it will account for 15% to 20% of my [organization's] managed security services revenue by the end of next year." Large, regulated customers, especially in healthcare and financial services, are adopting managed compliance as a service to outsource policy enforcement and reporting.

> "Our managed [Microsoft] Purview offering is our strongest growth area. … Demand is highest among large, regulated customers, and project scope has increased 30% to 40%."
>
> **DIRECTOR OF SECURITY, SYSTEMS INTEGRATOR**

Data Security And Compliance Opportunity



> "We see a lot of attention and focus on data security. … Compliance monitoring has become a big moneymaker. Customers want their data quality and mapping in order before investing in AI."
>
> HEAD OF SECURITY SERVICES, SYSTEMS INTEGRATOR

IDENTITY

IAM is now a foundation for AI, security, and modern work efforts. The surging demand for identity solutions doesn't just reflect advances in AI but establishes the integral role of Identity and Zero Trust in comprehensive security strategies. Partners emphasized that identity governance, which is increasingly bundled with data security and compliance offerings, is becoming critical for enabling secure AI adoption and managing agent lifecycle. Identity is seen as the "control plane" for AI security, covering conditional access, agent identity, and data access controls. This has led to growing interest in Microsoft's Identity solutions, especially in enterprise and regulated sectors.

Organizations are increasingly moving away from point solutions, which require more personnel for management and may come with higher/redundant licensing costs. Microsoft Entra ID has become a preferred choice for SSO solutions, as shown by SAP's recommendation that its customers adopt Microsoft Entra ID. Partners claimed that the adoption of Zero Trust frameworks is accelerating as their clients recognize the need for continuous verification and least-privilege access. Microsoft Defender solutions, particularly Microsoft Defender for Identity, are playing a key role by providing actionable insights into identity risks, helping partners make smarter, data-driven decisions about access control and threat mitigation.

> "Identity is linked to everything we do. There are still basic things like MFA and conditional access, but we are seeing more complex opportunities. … Do more with less is still a consistent theme here, leading to competitive takeouts."
>
> CHIEF COMMERCIAL OFFICER, SYSTEMS INTEGRATOR

- **Partners are still embarking on full identity deployment journeys, which can be multiyear and multimillion-dollar projects.** The shift away from point solutions is continuing to drive growth in identity deployment opportunities. The growing interest in Microsoft Entra ID governance is also driving more deployments as well as downstream

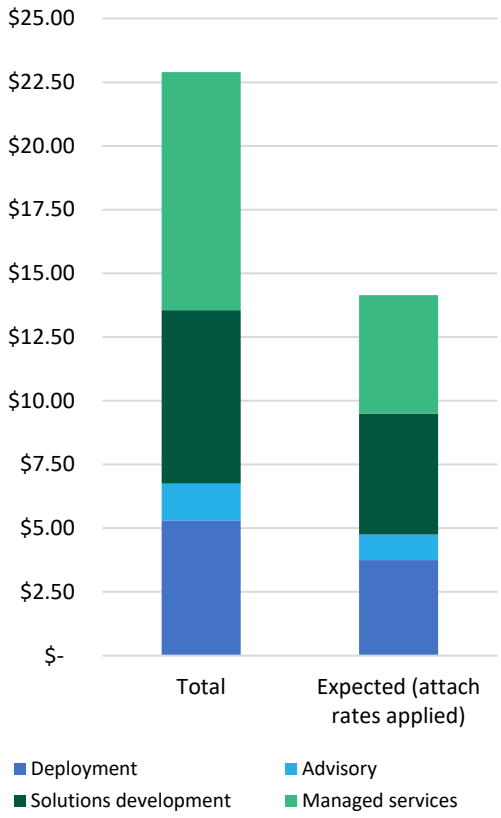
managed services opportunities for partners to provide more comprehensive identity services.

- **Advisory services' attached revenue opportunity grew by 25%.** Identity opportunities are embedded across partner security services. One partner said, "Identity is the first thing we put on the roadmap." Another partner told Forrester, "We are seeing that identity opportunities are becoming more complex, with companies undergoing acquisition and looking to streamline security across domains."
- **Custom solutions enable partners to provide more extensive identity security monitoring.** Partners have developed identity connectors, security IP, and business solutions to enhance their identity services. These services encompass both cloud and on-premises identity monitoring and incorporate telemetry into a SOC. One partner built a migration tool for competitive takeout scenarios for identity solutions, a part of the broader data security and compliance motion.
- **Partners are extending their identity managed services with Microsoft Entra ID Governance.** The managed services opportunity for Identity spiked over the past 15 months. Interest in Microsoft Entra ID Governance is rising, enhancing go-to-market strategies and fostering the development of new identity monitoring solutions. This trend is driving managed services revenue growth: One partner anticipates a 10% to 20% increase in deal size due to the heightened focus on identity governance solutions.

"We're noticing a significant number of customers taking identity governance really seriously. That's a marked shift from the past. … All the interest in agentic AI is absolutely driving more focus on security and the need for data and identity security across our clients."

DIRECTOR OF SECURITY, SYSTEMS INTEGRATOR

Identity Opportunity



XDR

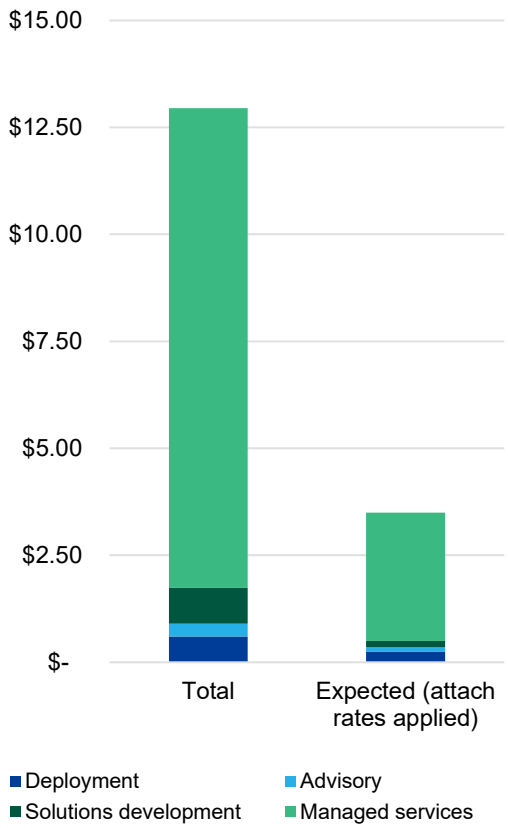
Clients face more and increasingly complex vulnerabilities, which presents a significant growth opportunity for partners. The demand for comprehensive cybersecurity solutions is driving double-digit growth in managed detection and response (MDR) and XDR services. This growth is particularly notable in the SMC market, where smaller companies often lack the resources to maintain a SOC. The maturity of managed XDR (MXDR) offerings makes it challenging for these organizations to fund in-house security teams, creating a lucrative opportunity for partners. One partner said: “A lot of signals are coming in. If you use an SOC in combination with [Microsoft] Defender, then you can reduce noise and false positives. Additionally, our analysts have a single pane of glass.” This allows partners to reduce complexity and create a shared model of MXDR services.

Despite the growth and higher margins in the MXDR space, competition is increasing, which is beginning to lead to downward pricing pressure in some geographies. Forrester found that partners without dedicated MXDR services have created success by reselling or private-labeling other partners' MXDR offerings. One partner established just such a relationship after being connected by Microsoft's partner organization.

- **The expected revenue opportunity for deployment grew by 25%.** While XDR services primarily focus on managed services, partners are seeing more deals and high profitability for implementation projects, including upfront workshops and deployment. Partners generate new business through XDR-related presales engagements, which Microsoft sometimes funds.
- **Advisory services play an important role in setting customers up for long-term success.** These services typically include defining the managed services model, establishing clear interaction frameworks between the partner and the customer, and creating a baseline of the customer's security posture to support effective incident response. In addition, partners often provide IT and end-user training to strengthen security awareness, reduce the number of detection and response activities, and improve operational efficiency and profitability.
- **Partners offer bespoke incident response services beyond a retainer.** Incident response is classified under custom solutions due to the bespoke nature of the work. Partners stressed the importance of preventing incidents through proactive protection and rapid detection. While more partners are charging incident response retainers, they often describe large remediation projects as stressful and operationally burdensome. Consequently, partners prefer to focus their sales efforts on proactive services (to avoid incidents), which offer higher margins and are less operationally intensive. The head of security services at a systems integrator told Forrester, "One hundred percent of [incident response] projects transition into other work. Every single one has some kind of service retainer afterwards."
- **Managed services opportunities with XDR grew by 50%.** Partners told Forrester that MXDR allows them to provide proactive services that lead to higher retention and margins. The combination of Microsoft Sentinel, Microsoft Defender XDR suite, and Azure Arc enables partners to provide unified MDR solutions across various platforms and workloads, effectively addressing clients' diverse needs. The integration of multiple signals with SOCs also helps eliminate false positives, giving analysts a unified view and reducing operational costs.

- **Partner-to-partner relationships are on the rise as partners seek to enhance their offerings.** This is particularly evident in the managed services for MXDR space, where collaboration helps round out service portfolios and meet customer demands. Additionally, white-labeling offerings help partners expand their addressable market. To serve this customer segment cost effectively, partners are developing streamlined solutions and increasing automation in service delivery, using tools like Microsoft Security Copilot or other agentic AI solutions developed with Microsoft. Partners are reporting improved automation and security ticketing efficiency gains between 60% to 85%. One partner noted that Security Copilot now automates 80% of help desk tickets, boosting the managed services team's efficiency by 40%.

XDR Opportunity



“We are seeing significant growth in MXDR services. Our recurring revenue growth is just short of 40%.”

CYBERSECURITY AND INNOVATION STRATEGY LEADER, SYSTEMS INTEGRATOR

PARTNER INVESTMENTS AND BEST PRACTICES

Each year, Forrester asks representatives of partner organizations about the new best practices and investments fueling their success with go-to-market approaches and delivery. This year, partners mostly spoke about what they are doing to succeed in the new AI-first environment. They said they are:

- **Increasing automation to deliver managed SOC and MXDR.** Partners with strong managed services said that they are investing heavily in automation to improve their services, reduce their cost of delivery, protect margins, and scale services. Some European partners said that they are seeing downward pricing pressure in managed services, so becoming more efficient is imperative. Partners also said that more automation was very important in order to serve the SMB/SMC market profitably. Partners that use Security Copilot effectively, typically in conjunction with Microsoft Sentinel and/or Microsoft 365 Lighthouse, reported large improvements in terms of automating ticket responses and reducing security analysts’ manual efforts. Partners that did not have their own managed SOC or MXDR offerings were increasingly reselling other partners’ services. One partner that specializes in MXDR said: “We started reselling our services through other partners, which drove $1 million in revenue last year. We have since hired someone to manage our own channel.”

> "We've automated 83% of incidents. … We're doing more with customers with less staff. In the last 12 months when someone's resigned or immigrated, we haven't replaced them."
>
> CEO, MANAGED SERVICES PROVIDER

> "We use [Microsoft 365] Lighthouse and [Microsoft] Sentinel to deliver all of our managed services. Without them, we couldn't deliver our services and be price-competitive."
>
> MICROSOFT SECURITY LEAD, SYSTEMS INTEGRATOR

- **Focusing on the E3 to E5 security story in support of AI readiness.** Partners had previously pitched to customers the security benefits of moving to Microsoft 365 E5, either the full E5 SKU or the Defender Suite or Purview Suite add-ons, but customers' desire to be AI-ready has made them more receptive to the conversation and making the move. Implementing the add-on solutions can significantly increase revenue across all partner solution areas, deployment, advisory, business solutions, and managed services. Partners that don't have the expertise necessary to support the various Microsoft 365 E5 solutions are investing heavily in developing those capabilities in-house or are working with other Microsoft partners to deliver services like managed SOC and MXDR.

> “Customers have a much greater appreciation that they need [Microsoft 365] E5 now. The great thing for us is that it includes a lot of capabilities customers don’t have the resources to support. This can lead to managed SOC and other managed services conversations.”
>
> MICROSOFT SECURITY LEAD, SYSTEMS INTEGRATOR

- **Restructuring to provide more holistic support.** Partners are rethinking how they are structured in terms of sales and delivery in order to provide customers with all of the knowledge and services required to fully support their AI journeys. How partners are restructuring varies greatly: Some have created virtual teams that cross practice areas, while others have fully reorganized to create unified AI delivery teams. Many partners are investing in cross training and coordinating delivery resources across Microsoft practices, such as security, modern work, and Azure, to deliver integrated solutions, especially for AI-driven scenarios.

> “We intentionally didn’t replace some of the people who left. … The skill differences between a modern work human and a security human have shrunk. The automation has dramatically increased.”
>
> PRESIDENT, CLOUD SOLUTIONS PROVIDER

> "We've had to rethink how we work because customers are trying to solve a business problem with AI, not implement technology. By bringing our teams together, we can better understand and support our customers."
>
> COFOUNDER AND EXECUTIVE DIRECTOR, SYSTEMS INTEGRATOR

- **Creating or strengthening advisory capabilities to support customers' AI journeys.** Some partners said they lacked comprehensive advisory capabilities that bring together business and technology acumen to help customers become AI-ready. Securing information is as much about process and governance as it is about technology. Customers see the value of advisory services and are willing to pay for them when it comes to AI, so partners are adapting in order to take advantage of this increased revenue opportunity. This includes hiring for roles like business analyst and data scientist as well as investing in delivery and training capabilities. One partner chose not to invest in building out all these capabilities but partnered with another Microsoft partner instead.

> "With respect to AI, it is all about laying the right foundations, which requires a lot of adoption and change management consulting. We don't do this ourselves, so we partnered with a specialized agile change management consultancy. We refer a lot opportunities to each other."
>
> CHIEF COMMERCIAL OFFICER, SYSTEMS INTEGRATOR

- **Working more closely with Microsoft to maximize AI opportunities.** Partners said that aligning closely with Microsoft is more important now than ever before. This includes product and service alignment, marketing messaging, co-sell activities, partner

engagements, and being enrolled as a Microsoft AI Cloud Partner Program (MAICPP) with a Security Designation. They also said it was important to obtain all four Microsoft Security Specializations: Cloud Security, Information Protection and Governance, Identity and Access Management, and Threat Protection.

> "We have a very clean product and service alignment with the Microsoft security stack, which makes it easier for us to collaborate with Microsoft and to leverage available funding. This approach has been incredibly successful for us. Probably 50% of our new business comes from funded workshops [partner engagements]."
>
> CHIEF COMMERCIAL OFFICER, SYSTEMS INTEGRATOR

- **Introducing transactable marketplace offerings.** While many partners with marketplace offerings reported this primarily helps with marketing, market education, and lead generation, several partners shared they are seeing revenue from transactable marketplace offerings. Productized IP and managed services allowed these partners to expand global reach without adding operational overhead. The CEO of a managed service provider told Forrester: "We've moved a lot of our offerings into the Azure marketplace. So it's made it much easier for customers to interact with us outside of our traditional markets."

> "We've been capable of delivering two transactable offers … selling managed services or IP as if it was software. … That offers us a global reach and a revenue stream on top of our investments without additional operational costs."
>
> HEAD OF SECURITY SERVICES, SYSTEMS INTEGRATOR

Conclusion

The 20% growth in expected revenue since FY 2024 was substantially more than the 10% growth achieved in FY 2024. In large part, this is attributable to customers' interest in adopting AI. The most direct impact was on Data Security and Compliance, which is central to AI readiness. The other solution areas also saw strong growth because of AI as well as the increased complexity of cyberattacks and customers' desire to reduce costs through vendor consolidation.

The two partner service areas that experienced the largest growth in percentage terms were advisory and managed services. AI has created a large opportunity for advisory services that help customers get AI-ready. Managed services opportunities continue to grow as companies deal with shortages of IT and IT security professionals. Managed services increasingly include the MXDR services that partners have launched to tackle multivector threats. Setting up and providing an industry-leading MXDR offering requires a lot of investment, so many partners are choosing to resell other partners' XDR services. Expected revenue for XDR managed services increased by 50%.

Partners believe that this year's successes will continue and grow in the remainder of FY 2026 and beyond. Agentic AI should be a main driver of growth, especially in Identity. Microsoft's ongoing investment in security-related solutions, marketing, and partner programs will create more and larger opportunities for partners. The partners applying the best practices described in this study are experiencing the largest success, and this will continue to be the case in the years to come.

APPENDIX A: TOTAL ECONOMIC IMPACT

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

APPENDIX B: ENDNOTES

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[2] An attach rate is the likelihood of a given service/solution being included in what a customer purchases. Attach rates are applied to solution areas (e.g., Microsoft 365 Security, Multicloud Security, Data Security and Compliance, Identity, and XDR) and to services (e.g., deployment, advisory, business solutions, and managed services). In other words, they're applied to the typical mix of solutions and services a customer buys. This will vary based on how a partner has entered into security. For example, a compliance partner will attach a lot more data security and compliance, while a managed security services provider will attach a lot more Microsoft 365 security. Use this calculation: total opportunity x attach rate = expected opportunity.

[3] Source: "The Microsoft CSP Partner Security Opportunity Analysis," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, August 2025.

[4] Source: "The Impact of AI On Microsoft Modern Work Partner Revenue: Copilot And Agents," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, July 2025.

[5] Source: The State Of Technology Services, 2025, Part 1: Co-Innovation Services, Forrester Research, Inc., March 18, 2025.

[6] Source: Forrester's Priorities Survey, 2025.

[7] Source: Forrester's Security Survey, 2024.

[8] Source: Forrester's Priorities Survey, 2025.

[9] Source: Forrester's Industry- And Customer-Supporting Software Survey, 2025.

[10] Source: Forrester's Priorities Survey, 2025.

[11] Source: Forrester's Industry- And Customer-Supporting Software Survey, 2025.

FORRESTER®