

The Partner Opportunity For Microsoft Security

A Total Economic Impact™ Partner Opportunity Analysis

A FORRESTER TOTAL ECONOMIC IMPACT STUDY
COMMISSIONED BY MICROSOFT, JUNE 2024

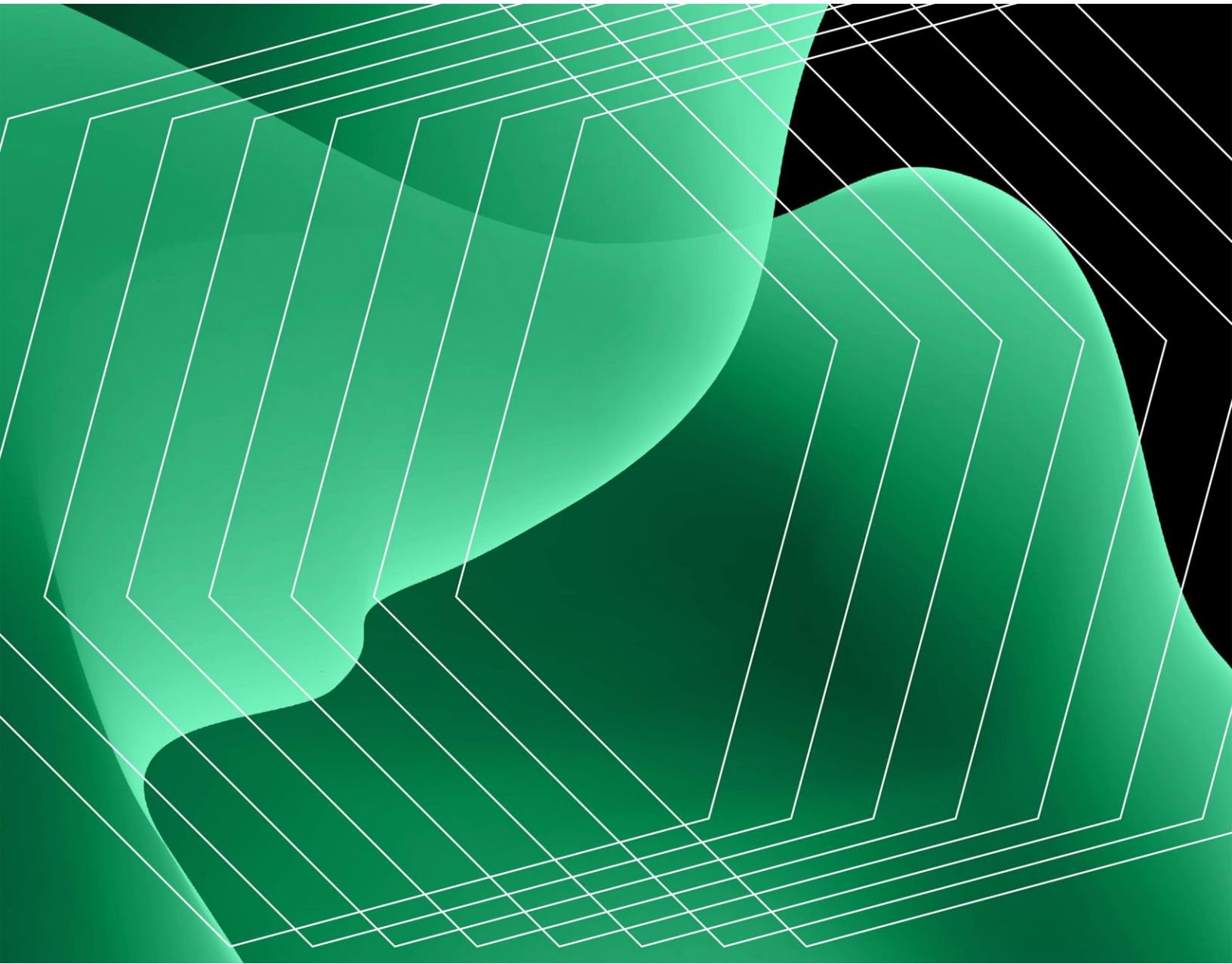


Table Of Contents

Introduction	3
Market Trends	7
The Partner Opportunity For Enterprise Customers	13
The Partner Opportunity For SMB Customers	25
Partner Investments And Best Practices	31
Conclusion	33

Consulting Team:

Luca Son

Marianne Friis

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.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Introduction

The partner opportunity to deliver services and solutions related to Microsoft security grew in fiscal year (FY) 2024 by 10% at enterprise customers and by 19% at small and medium-sized business (SMB) customers. This growth was driven by several factors, including customers getting ready for generative AI, customers' desire to reduce costs while improving IT security, and partners expanding into new solution areas in response to Microsoft's increased investments in its security-related offerings. Partners that invested in their internal capabilities and Microsoft relationships reported higher revenues and profitability.

Many factors contributed to the increased partner opportunities to assist customers with their security and compliance needs. First and foremost, the meteoric rise in customer interest to use generative AI (genAI) solutions in the workplace and the launch of Copilot for Microsoft 365 mean organizations that previously deferred security and compliance work must now make up for years of underinvestment. Second, cyberthreats continue to increase in terms of complexity, frequency, and notoriety. In part, this is due to bad actors using genAI to increase the sophistication and perceived believability of attacks across existing and new threat channels. Third, ongoing economic uncertainty has spurred companies to look for ways to reduce costs. In many cases, companies are double-paying for security solutions in the form of Microsoft premium SKUs (Microsoft 365 E5 for enterprise customers and Microsoft Business Premium for SMB customers) and point solutions from other IT security vendors. CFOs are asking their IT organizations if the same (or better) level of security and compliance protection can be achieved while rationalizing the IT estate. Lastly, Microsoft's ongoing investments have made it easier for partners to expand into new solution areas and for partners with established practices to go deeper with their customers. This has also contributed to more success in selling and delivering ongoing managed services.

In order to understand the impact of the above trends, 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 for both enterprise and SMB customers.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 Purview, and Microsoft Priva.

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

- **Microsoft 365 Security.** This solution area covers activating and managing everything security-related in Microsoft 365, including security operations center (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’ infrastructures, apps, and data.
- **Compliance.** Microsoft Compliance capabilities include data security (information protection, data loss prevention, and insider risk management) and governance and privacy.
- **Identity.** Identity and access management (IAM) includes providing core digital identities to knowledge and frontline workers as well as to third parties, Microsoft Entra ID, Zero Trust initiatives, and capabilities such as single sign-on (SSO) and multifactor authentication (MFA).
- **XDR.** XDR is primarily a proactive managed services opportunity and a natural extension from endpoint detection and response (EDR). 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.

Enterprise customer expected revenue opportunity (with attach rates applied)

\$45.30 per user per month

SMB customer expected revenue opportunity (with attach rates applied)

\$17.70 per user per month

*Based on a 36-month customer journey.

This year's study focuses on what has changed for security partners in FY 2024 and the outlook for FY 2025. This includes: 1) what customers look for from Microsoft partners; 2) how partners make money; and 3) the best practices and investments that create success.

To better understand the revenue streams and investments associated with a Microsoft security practice, Forrester interviewed representatives from 13 partners with practices in one or more of the aforementioned solutions areas. It also includes the partners' security-related data from another TEI study focused on the partner opportunity for Microsoft Modern Work.² These interviews build on more than 65 interviews with Microsoft partners that were conducted in previous years, as well as dozens of organizations consuming partners' services.

Forrester created partner-opportunity models for both enterprise and SMB customers based on what leading partners achieved in FY 2024 and what they expect to achieve in FY 2025. These models quantify the opportunities for deployment, advisory and adoption services, solutions development (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 10% year-over-year (YoY), and that the SMB revenue opportunity is up by 19% YoY.³

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.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Microsoft and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in a Microsoft security practice.

Microsoft reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Microsoft provided the partner names for the interviews but did not participate in the interviews.

1. Due Dilligence

Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Security.

2. Interviews

Interviewed representatives at 13 partner organizations with one or more existing Microsoft 365 Security, Multicloud Security, Compliance, Identity, or XDR practices to obtain data with respect to revenue opportunities, investments, and best practices.

3. 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 during a 36-month customer journey.

4. Case Study

Created a case study that explains the benefits and investments a partner can expect when building one or more security practices. The case study also explores the best practices partners have identified, which have made them successful.

Market Trends

THE CUSTOMER PERSPECTIVE

This section incorporates some of Forrester analysts' research and Forrester Analytics Global Business Technographics® survey data to understand what is driving customer demand in terms of the services they are looking for and from whom they want to buy these services. In Forrester's Security Survey, 2023, 27% of security decision-makers said that their organization's top IT priority is to improve security and privacy.⁴ In the same survey, 70% of security decision-makers with decision-making power at the manager level or higher shared that their IT budget for security increased from the previous year.⁵ Additionally, IT services budgets are expected to grow by 4% in 2024, with security being one of the largest investment areas.⁶

Software-as-a-service (SaaS) adoption also continues to be a major driver of security services adoption. In a 2023 Forrester survey of 2,670 software decision-makers, 28% said data security and protection against cybercrime were their organization's biggest concerns with using SaaS solutions.⁷ Additionally, Forrester's Security Survey, 2023, of 3,024 security decision-makers found that 14% of respondents expect the largest portion of their organization's security budget will go to existing security technology.⁸ The survey also revealed why organizations are looking to outsource security services. Security decision-makers outlined the following top priorities: improving quality of protection (40%), increasing competency or specialized skills (33%), and improving regulatory compliance (33%).⁹

Security technology decision-makers also noted their organizations' top security priorities for the following 12 months. Microsoft solutions and the related partner opportunities align with most of the top 10 priorities, as seen in the table below.

IT Security Priorities	
Improving application security capabilities and services	25%
Improving threat intelligence capabilities to proactively identify security threats targeted to my organization or industry	23%
Improving access management tools and policies for employees and partners	23%
Improving data security capabilities, such as identification and classification	22%
Using built-in security capabilities from Microsoft, Google, AWS, etc.	21%
Improving security operations effectiveness	21%
Improving vulnerability risk management capabilities and process	21%
Improving security communications and security awareness and training	21%
Improving device security and services to support anywhere work	20%
Improving endpoint security capabilities and services	20%
Move security solutions to the cloud	18%

Lastly, the reasons security decision-makers said they purchased IAM technologies for their organizations during the previous 12 months represent a large opportunity for partners to deploy and manage solutions. The top four drivers were replacing or enhancing a commercial IAM solution (26%), improving customer experience during the customer journey (26%), regulatory compliance (25%), and cloud migration that required new IAM solutions (25%).¹⁰

THE PARTNER PERSPECTIVE

Partners shared their views on the high-level trends driving opportunities and what they believe will be even more important during the next year. These include:

- **Generative AI is creating opportunities and increasing threats.** Interviewed partners all said that the rise of generative AI and widespread customer interest in Copilot for Microsoft 365 is creating a lot of buzz and opportunity. One of the main components of becoming AI-ready is defining and implementing proper data security governance and controls. This is something that many customers put off in the past but can no longer ignore. Some partners are beginning to use Copilot for Security as part of their services, and they expect it to improve managed services efficiencies.

“We are doing a lot of Copilot-readiness assessments. If you turn Copilot on without doing proper planning, it can create information governance and protection issues. We are also helping our customers figure out what responsible AI looks like.”

- **Microsoft security is more than a platform — it is a collection of best-in-breed solutions.** Partners reported that IT leaders at their customers are under increased pressure to reduce costs while maintaining — or ideally, improving — the security posture. Microsoft security solutions are a good area to look at for cost reduction/vendor consolidation to reduce license costs, in-house IT effort, and multiple professional services contracts. Partners also said that their customers are increasingly willing to consider consolidating onto Microsoft as the solutions have matured and because the individual solutions are often rated industry-leading by analyst firms.

“Microsoft invests more in R&D than everyone else combined. Their integrations and multisystem signal ingestion improve security. If a customer goes with best-of-breed solutions from multiple vendors, it increases their costs and their security risks because of possible misconfigurations and configuration drift.”

- **IT and IT security skill shortages are increasing, which creates more managed services opportunities.** The shortage of IT security professionals in the workforce continues to be a challenge for most companies. This is especially true in the SMB market. Partners said that their customers increasingly depend on Microsoft partners to fill the skills gap, creating many more managed services opportunities.

“Companies can’t hire enough personnel to manage their security solutions or to do the actual detection, analysis, and remediation work. We help customers overcome this by moving them fully onto the Microsoft solution stack and then managing everything for them.”

- **The SMB opportunity continues to expand rapidly.** This is the second year in which partners have spoken enthusiastically about the growth in SMB. This is driven by the previously discussed need to do more with less in terms of dollars

and people and by Microsoft's continued investment in solutions that are right-sized for the SMB market. Additionally, SMBs have greater awareness that they are targets of malicious actors. Many partners that previously sold only to enterprise customers are now selling to the upper end of the SMB market. Partners that exclusively focus on SMBs have benefited from more managed services opportunities, which grew 53% in FY 2024 for SMB customers versus 17% for enterprise customers.

"There are 1.3 million SMBs in the US. Although there are still a lot in denial, most companies know someone in their space who has had an incident or breach. That is our growth engine."

- **Partners are moving into new solution areas and making greater use of Microsoft Sentinel.** The breadth of capabilities in the hero SKUs Microsoft 365 E5 and Microsoft 365 Business Premium are making it easier for security partners to build and demonstrate competencies in new areas such as Compliance and Multicloud Security. Furthermore, more partners are using Microsoft Sentinel and increasing the number of integrations to provide managed services such as managed SOC and managed XDR. Partners that lack in-house capabilities to deliver these managed services are more often reselling/white-labeling other partners' managed services. Taken altogether, increases the total potential revenues at any given customer through a land-and-expand strategy.

“Our total addressable market is all the companies using Microsoft 365 E5. Microsoft’s success in getting these companies to use the various security solutions has helped us get greater market penetration and grow as an MSSP.”

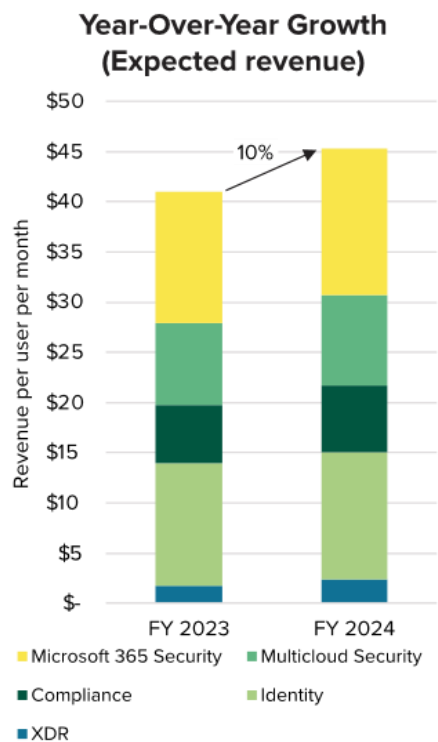
- **Microsoft’s delivery and co-selling/co-marketing programs are driving success.** Partners continue to take advantage of Microsoft funding for pilots and proofs of concept (POCs) to jumpstart projects in new solution areas. Additionally, partners reported making more use of Microsoft resources for sales and marketing activities and in project delivery. These are all helping partners to expand into new solution areas, enter new markets, and grow top-line revenues.

“Microsoft’s programs are extremely important to our business. We have a team dedicated to working Microsoft on co-selling and co-marketing. It is a big driver of our revenue.”

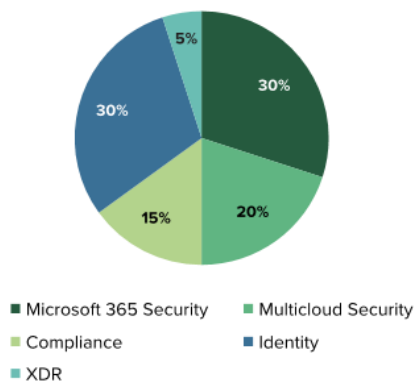
The Partner Opportunity For Enterprise Customers

ENTERPRISE OPPORTUNITY OVERVIEW

The trends discussed above resulted in increased revenues across all solution areas in FY 2024, 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 customers are buying (attach rates applied). The expected revenue opportunity grew by 10% for an enterprise customer on a three-year journey. While Microsoft has a mature partner ecosystem, partners signaled that Copilot for Microsoft 365 and Copilot for Security are expected to drive future growth. The two solution areas with the largest year-over-year expected revenue growth opportunities are Compliance and XDR, in part driven by generative AI opportunities.



Attached 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 8%.** Deployments are the typical entry point for new customer engagements. Partners viewed deployments as a consistent way to drive new business that can later evolve into advisory and managed services opportunities. Deployment opportunities remain a growth area in FY 2024 as customers continue to grow their cloud footprint and transition to Multicloud Security. Forrester found an increased interest in vendor consolidation as the Microsoft portfolio converges to best of breed in capabilities and connectivity, and as security decision-makers increasingly focus on lowering total cost of ownership (TCO).
- **Advisory services grew by 15%.** Partners are offering more advisory services to prepare customers for growing complexity in the threat landscape and to ensure successful adoption of a comprehensive security strategy. Advisory services are critical to prepare customers for increasingly sophisticated attacks that incorporate genAI, as well as new genAI security solutions like Microsoft Copilot for Security. Advisory includes upfront strategy and planning work as well as adoption and change management (ACM) services. Advisory helps partners differentiate their services, improve the stickiness of their offerings, and increase security success.
- **Solutions development grew by 2%.** Solutions development includes the repeatable IP that partners create (either as standalone solutions for sale or used to make deployments and managed services more efficient), custom solutions development, and advanced integration work. Partners continue to offer custom integrations, particularly around compliance connectors.
- **Managed services grew by 17%.** Partners are focusing on their managed services, a key component to scaling and driving predictable business. Partners viewed managed services as a strategic offering to increase upsell, margins, and repeatable business. With Microsoft Copilot for Security, partners are expecting to improve operational efficiency and further improve margins. Partners are

building managed-compliance offerings as customers are preparing for genAI adoption.

Enterprise Customer Revenue Opportunity By Solution Area				
Solution area	Total revenue per user per month	Blended attach rate	Expected revenue per user per month	Expected YOY growth
Microsoft 365 Security	\$42.45	34%	\$14.60	11%
Multicloud Security	\$23.45	38%	\$9.00	10%
Compliance	\$20.35	33%	\$6.70	16%
Identity	\$21.35	59%	\$12.65	3%
XDR	\$11.65	20%	\$2.35	34%
Total	\$119.25	38%	\$45.30	10%

Enterprise Customer Revenue Opportunity By Partner Service				
Partner Service	Total revenue per user per month	Blended attach rate	Expected revenue per user per month	Expected YOY growth
Deployment	\$17.65	59%	\$10.40	8%
Advisory	\$6.80	50%	\$3.45	15%
Solutions development	\$40.80	31%	\$12.55	2%
Managed services	\$54.00	35%	\$18.90	17%
Total	\$119.25	38%	\$45.30	10%

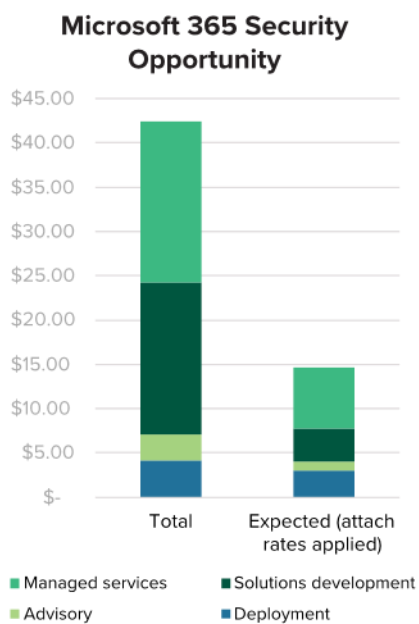
MICROSOFT 365 SECURITY

Microsoft 365 Security is about activating and managing Microsoft 365 solutions securely. Customers are confronting an evolving threat landscape, leading to greater security solution deployments. Gaps in security tooling are becoming more evident. New capabilities and connectors with the E5 SKU are driving increased E3-to-E5 upgrade and competitor takeout opportunities.

- **Deployment services were driven by an increase in vendor consolidation opportunities.** Forrester found a shift in strategic focus from a best-of-breed approach toward vendor consolidation, driven by broadening capabilities from Microsoft, improved interoperability, simplified management, and cost savings. Partners saw an increase in competitive takeout opportunities. Presale engagements and End Customer Investment Funds (ECIF) funding are driving

new opportunities and follow-on work. Partners continue to help customers build out their SIEM and SOC capabilities.

- **The largest growth was in advisory services, representing a 9% uplift compared to FY 2023 and a 33% attach rate.** Partners told Forrester that upfront strategy and planning were essential to set organizations up for success and maximize further investments in solution development and managed services. The evolving complexity of threats and the broadening of the Microsoft 365 Security portfolio with Copilot drives advisory opportunities.
- **Custom solutions offering drive extensibility and more ingestion points for SIEMs.** Solution 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. Partners also do custom integration work to help customers build out their Microsoft Sentinel-based SIEMs.
- **Managed services opportunity is attaching at higher rates.** Managed services opportunity attached at 38%, as partners increasingly focus sales activities on accounts that can result in managed services. Managed services are an attractive offering for customers that struggle hiring talent and building in-house expertise to address the changing threat landscape.



“The more solutions Microsoft releases, the bigger our opportunity. Even if a customer is already on E5 and deployed all the Defenders, new features drive growth.”

MULTICLOUD SECURITY

Multicloud Security includes the services and solutions partners offer around Azure and other public clouds that run Microsoft solutions. While hybrid is here to stay, the continuing trend of migrating to the cloud creates new and expanded opportunities. Partners are building Azure capabilities to support what is seen as a growth area. Partners viewed Defender for Cloud as “ready for prime time.” Multicloud continues to create XDR opportunities.

- **Expected deployment revenue grew 13%.** While deployment projects for Azure, Defender for Cloud, and others typically begin with a POC or security assessment, deployment work accounts for a much greater percentage of revenue. Partners offer Azure server migration, Azure application migration, and Azure migration and transformation security work. Most partners focus on Azure deployments but are equipped to support customers on other public clouds.
- **Advisory work helps customers move securely to the cloud.** Partners offer Azure security strategy, planning, and upfront governance work to ensure a successful cloud migration. Expected revenue grew by 7% as customers continued to migrate to the cloud.
- **Partners create their own solutions for securing cloud operations.** Complex migration work opens the opportunities for partners to offer custom solutions, whether packaged through Azure Marketplace or bundled into migration and managed services. Custom IP helps increase revenue potential and margins.

- **Managed services are increasingly including multicloud security.** Expected revenue for managed services grew 16%. Partners continue to help customers operate securely in the cloud as IT expertise remains in short supply. Pricing can be based on a customer's annual cloud consumption spend or on a per user, per month basis.



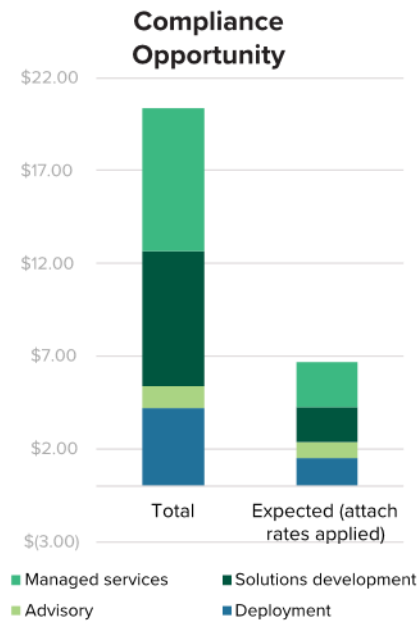
“10% to 20% of our overall data-center-to-Azure migration is security related. Defender for cloud is easier to enable and has automation and monitoring built in. Customers see the value.”

COMPLIANCE

Compliance was the fastest-growing solution area in expected opportunity and is an adjacent area to security where partners seek to create new offerings. Copilot for Microsoft 365 has made compliance a top priority for nearly every company. Customers are eager to adopt Copilot for Microsoft 365, which gives partners the opportunity to provide compliance deployment, advisory, solutions, and managed services to prepare them for genAI adoption. Insider risk opportunities have grown significantly due to the introduction of Copilot for Microsoft 365, increased regulatory and reporting requirements, and because it is the next step in a compliance customer journey. More partners can move into compliance because the E5 SKU makes it easier for them to create competencies. Specialized partners continue to offer services around regulatory/legal and privacy that require deeper skills than most general security partners have.

- **Deployment saw an 8% growth in revenue opportunity.** Most customers begin their journey in areas closer to IT security, such as information protection and data loss protection (DLP). Partners are increasing their compliance solutions setup and seeing large e-discovery setup and migration opportunities.
- **Advisory services are attaching at 71%.** Partners saw compliance as a sticky offering. Deployment opportunities gave way to greater cross-sell activities and follow-on work, particularly around advisory and managed services. Partners offered a new genAI-readiness advisory solution, which is already attaching at 35%. Governance was a big part of the upfront work.
- **Partners build and sell solutions that streamline compliance management.** Partners built solutions to make compliance offerings easier to manage and more effective for customers. Partners offered information protection governance, e-discovery business, and compliance connector solutions.
- **Security partners are offering more compliance managed services.** Partners said they are building compliance-as-a-service offerings that parallel their security managed services offerings; they also noted that attach rates are increasing. Customer needs are always evolving. Partners offering compliance services were well positioned to increase follow-up work and provide managed

services around DLP monitoring and compliance alerting. More specialized partners are providing e-discovery managed services.

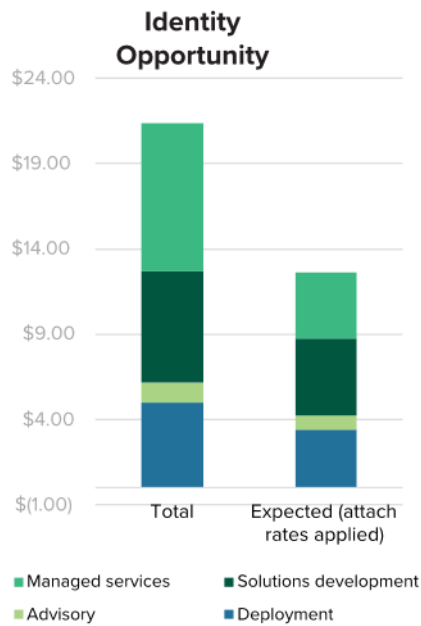


“Cross-selling is high with our compliance offerings. When you are getting client telemetry, that tells you the clients’ systems and business protocols, then you have the permission to have the discussion with clients’ own data as a sales conversation. It feeds the strategy and roadmap.”

IDENTITY

IAM is a fundamental component to all of security, compliance, and broader modern work efforts. Partners view identity as a mature area, but there are untapped opportunities in frontline workers and in markets outside of the US. Partners saw a spike in competitive takeout opportunities in areas such as SSO and MFA. These projects tend to be larger migrations than in past years. The Zero Trust story still resonates with customers and leads to device management opportunities.

- **Full identity deployment journeys can still be multiyear and multimillion-dollar projects.** New identity deployment opportunities are coming from competitive takeouts in SSO and MFA as organizations seek to control risk and reduce spend. The smallest projects were priced at \$50,000 but could range up to the multimillions of dollars.
- **Advisory services total revenue opportunity grew by 14%.** Identity impacts every user, so it is top of mind for customers. Advisory services for identity attached at 70%.
- **Custom solutions help partners offer more comprehensive identity security monitoring.** Partners built identity connectors, identity security IP, and identity business solutions to extend their identity offerings. These offerings cover both cloud and on-premises identity monitoring and integrate telemetry into a SOC. Custom integration work also ties to the Zero Trust security approach and messaging.
- **Identity managed services total revenue opportunity grew by 7%.** Identity-related managed services are often merged with broader L1 user help desk contracts. There are also managed services to ensure that all integrations are up to date and protect against configuration drift.



“Zero Trust still resonates. It gives us a good entry point to some of the other technologies that customers might not think of as identity.”

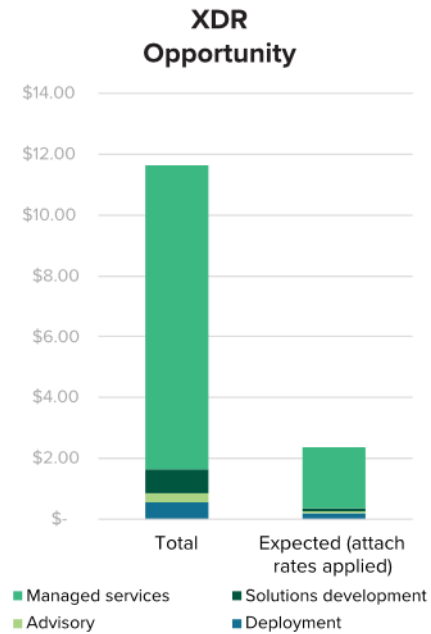
XDR

While XDR is a managed services opportunity, Forrester categorized this as a separate solution area. There is an upshift in customer demand for managed XDR (mXDR) due to solution improvements like more ingestion sources into Microsoft Sentinel and the need for comprehensive services that go beyond siloed threat protection. Partners increasingly say that the managed SOC landscape has become saturated and thus view XDR as a differentiator. That said, competition is increasing in the mXDR space, creating pricing pressures.

Partners spoke of mXDR as enterprise and midmarket customer opportunity. Large enterprises often have in-house capabilities, and pricing models is difficult at that size.

Forrester found an increase in partners reselling/private-labeling other partners' mXDR offerings.

- **Total deployment revenue opportunity grew by 33%.** XDR services revolve around managed services. Partners increase XDR opportunities by making upfront deployment seamless and a natural segue to managed services. Partners generate new business through XDR-related pre-sales engagements that are often funded by Microsoft and have seen an increase in win rates.
- **Advisory services help set up customers for success.** Advisory services include deployment advisory, defining the managed services model and interactions between the partner and customer, and baselining security posture for incident response. Partners also offer IT and end-user training to improve security posture and reduce ongoing detection and response work, increasing profitability.
- **Incident response is categorized under custom solutions due to the custom nature of the work.** Partners emphasized the importance of preventing incidents through proactive protection and detection. While more partners are charging incident response retainers, partners described large remediation projects as stressful and operationally burdensome. One partner had a zero-cost retainer so that a master service agreement (MSA) was in place.
- **Managed services pricing includes services contract and incident response retainer.** More and improved Microsoft Sentinel signal ingestion is increasing the number and size of new opportunities. Customers are asking partners for some form of monitoring, particularly if they are Sentinel customers. Partners see margins of around 50% when they implement automation and across-the-board protections for customers. Margins are expected to increase as investments taper and partners scale. Pricing varies depending on the types and volume of telemetry data being ingested. The more data partners can consume across identity, device, data, and application telemetry from hybrid environments, the better protection they can provide and the more they can charge.



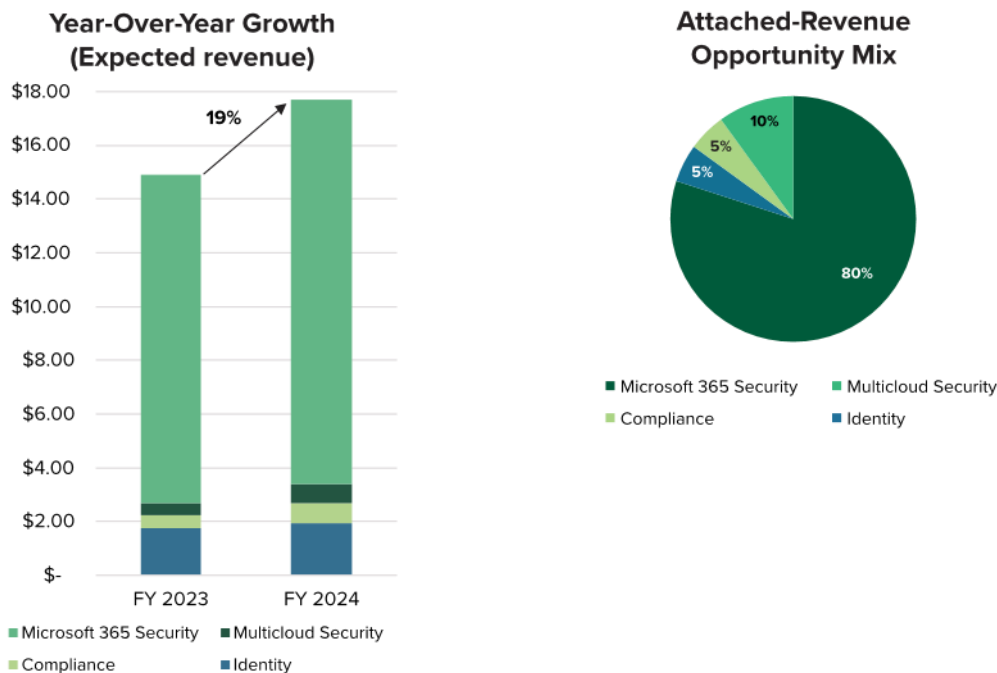
“Microsoft Sentinel ingests data points other platforms can’t. The number of changes and integration points in the last few years have been phenomenal.”

The Partner Opportunity For SMB Customers

SMB OPPORTUNITY OVERVIEW

Many trends discussed in the enterprise opportunity section also apply to the SMB opportunity. This section focuses on the differences among enterprise opportunities. In prior years, Forrester conducted the SMB security opportunity analysis as part of the modern work partner TEI study because the opportunity was almost exclusively around the Microsoft 365 Security and Microsoft Identity solutions. Since then, the SMB opportunity around Multicloud Security and Compliance has grown significantly. Therefore, this is the second year that the analysis has been expanded to include SMB in this study.

Overall, the SMB opportunity grew by 19% across Microsoft 365 Security, Multicloud Security, Compliance, and Identity solution areas. The XDR solution area is excluded from the SMB model because SMBs’ lesser requirements remain more of a managed SOC play.



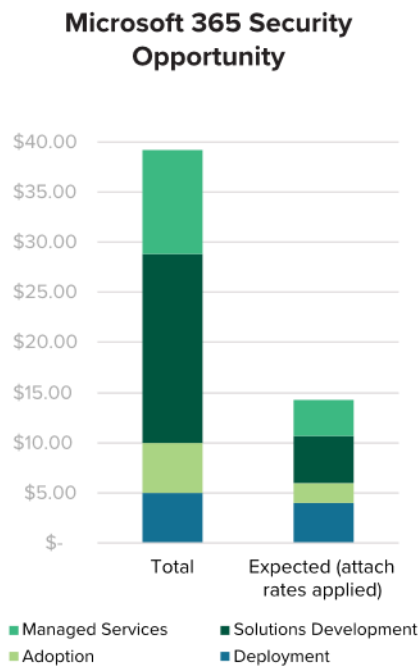
- **Deployment opportunities grew by 18%.** The increase in deployment opportunities was driven in part by more customers moving to Microsoft 365 Business Premium. Compliance and cyber insurance are incentivizing customers to adopt Business Premium. Compliance and Multicloud Security opportunities were more common for larger SMBs.
- **Adoption services grew by 13%.** For enterprise customers, adoption-related work is more basic and streamlined than advisory work. Adoption services are more prescriptive and provide more standardized training content and governance models.
- **Solutions development grew by 2%.** Partners create new IP they sell to customers or use to streamline their own deployment and managed services capabilities. Partners servicing SMBs operate leanly and spend less time on custom integration work than their enterprise counterparts.
- **Managed services grew by 53%.** Partners servicing SMB organizations focus predominantly on their managed services offerings. SMB organizations realize the increasing security threats to their organizations but lack the resources and expertise to build an in-house security team to manage threats.

SMB Customer Revenue Opportunity By Solution Area				
Solution area	Total revenue per user per month	Blended attach rate	Expected revenue per user per month	Expected YOY growth
Microsoft 365 Security	\$39.20	36%	\$14.30	17%
Multicloud Security	\$4.80	15%	\$0.70	56%
Compliance	\$3.20	23%	\$0.75	50%
Identity	\$4.90	40%	\$1.95	11%
XDR	NA	NA	NA	NA
Total	\$52.10	34%	\$17.70	19%

SMB Customer Revenue Opportunity By Partner Service				
Partner Service	Total revenue per user per month	Blended attach rate	Expected revenue per user per month	Expected YOY growth
Deployment	\$9.60	54%	\$5.20	18%
Adoption	\$5.70	39%	\$2.20	13%
Solutions development	\$21.00	26%	\$5.55	2%
Managed services	\$15.80	30%	\$4.75	53%
Total	\$52.10	34%	\$17.70	19%

MICROSOFT 365 SECURITY

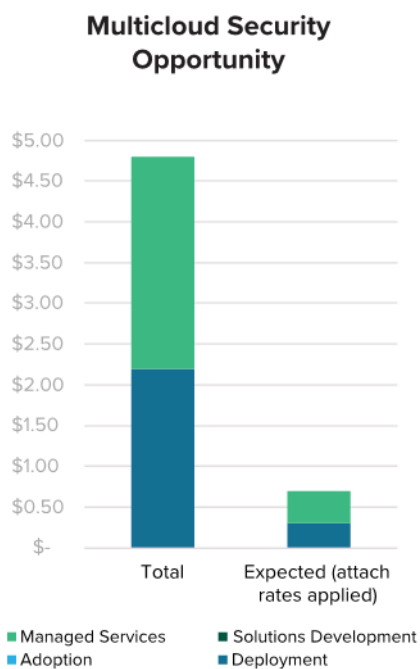
The increasing capabilities with Business Premium SKUs are increasing partners’ total addressable market. Organizations are reducing IT complexity and cost by moving to Microsoft 365 Business Premium. Upfront deployment work typically takes several days but can last as much as one month, depending on the organization size and feature requirements. Adoption services attach at 39%, and can include services like change management, external cybersecurity audits, or consultancy as part of managed security. Partners create solutions development to support managed service offerings. Partners offer a wide range of managed services offerings such as full IT security staff security and augmented managed SOC offerings.



“We lead with Microsoft 365 Business Premium because of the comprehensive suite of security tools. Ninety percent of our customers buy this SKU.”

MULTICLOUD SECURITY

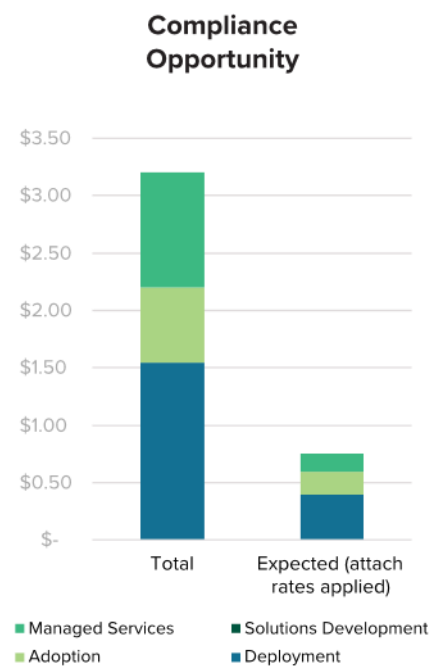
Partners are seeing more Multicloud Security opportunities at SMBs with 150 or more employees. Partners are recommending Azure adoption, which drives Multicloud Security opportunities. Deployment work is the security piece of an Azure migration. There are typically no separate adoption costs because this is built into the deployment services. There are no separate charges for solutions-development integration work because it is completed as part of the initial deployment, and management tools are priced into the managed services. Managed services ensure that proper security settings and Azure alerting are maintained.



“We help a lot of our new customers with cloud migrations, and they typically begin using Defender for Cloud to secure their cloud-based infrastructure.”

COMPLIANCE

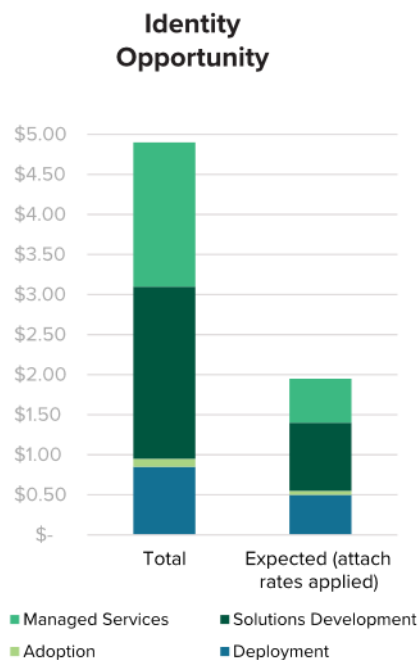
Compliance opportunities typically only exist for organizations with 150 employees or more, and they are primarily in data security. Compliance deployments usually take one to two weeks. Adoption services attach at 31% of the total compliance opportunity. There are no solutions-development offerings in terms of custom integration work. Partners offer managed services that attach at 15%. Partners that do not have compliance practices are increasingly referring or white-labeling other partners' compliance offerings.



“Our premium managed services offering uses Purview to deliver managed compliance.”

IDENTITY

Identity is central to the security work that partners provide SMBs. Deployment begins with enabling capabilities in Microsoft 365 Business Premium or in standalone security add-ons. Partners also help move customers to Microsoft solutions like SSO and MFA from other vendors. Partners provide basic training and templated content for adoption services. Partners that have created their own identity security tools for enterprise customers also sell them to SMBs. Identity managed services are included in full in IT and user-support outsourcing contracts.



“At SMB and SMC customers there is still a lot of identity-related cleanup work to do. We see a lot of shared accounts, which prevents them from implementing basic things like MFA.”

Partner Investments And Best Practices

Each year, Forrester asks representatives of partner organizations what new best practices and investments are fueling their success with go-to-market and delivery. This year, partners spoke about Copilot for Microsoft 365 adoption readiness; building out new offerings, particularly in the compliance space; and continuing to invest in their managed XDR services.

- **Adopt Copilot for Microsoft 365 and Copilot for Security.** Partners expressed enthusiasm and interest in the opportunities that genAI and Copilot would bring to their businesses. They emphasized the significance of adequately training and familiarizing their employees with Copilot to capitalize on growing customer interest and adoption opportunities. Additionally, partners highlighted the importance of providing sales and marketing training as it played a crucial role in educating customers and establishing realistic expectations.
- **Hire, train, and retain the best people.** Having the right talent is paramount to business success and is often the most difficult task for partners. IT and security professionals are in high demand and are becoming more costly with inflation, making hiring difficult. Employees require constant upgrading of skills and knowledge, which can be time-consuming and costly for partners to provide. Partners serving SMBs may have limited budgets for hiring and retaining IT and security personnel. This is why partners are conscious of investing in their employees and providing growth opportunities. Partners saw Copilot for Security as a solution to increase productivity and better use lower-skilled employees, which can help address labor shortage challenges.
- **Invest more in sales and marketing.** Partners focused on strengthening their sales and marketing capabilities. They recommended investing in training for account management teams to develop a better understanding of service portfolios and products. Several partners mentioned that becoming a trusted advisor helps create sales conversations at the C-level, leading to more deals.

- **Invest in customer success and customer experience.** Having the right personnel to speak to both technical and business challenges was key to helping partners become trusted advisors and to drive upsell and cross-sell opportunities.
- **Leverage Microsoft funding and programs.** Partners continue to take advantage of Microsoft programs. Although not all funding options for pre-sales engagements and pilots/POCs were viewed as equally good, the general consensus was that Microsoft funding helped win new accounts, expand into new solution areas and markets, and grow top-line revenues.
- **Focus on change management.** Partners said the key to deploying security and compliance and expanding into new solution areas is to understand business requirements and the impacts of the Microsoft solutions on business processes and people. Without this, the solutions will be less effective and seen as barriers to the business.
- **Going all in on Microsoft.** Many partners are 100% Microsoft shops or only do work in complementary areas with other vendors. Partners expressed that providing the bulk of their services within the Microsoft ecosystem improved integration and compatibility, centralized management, enhanced security and compliance, and resulted in additional support from Microsoft.
- **Standardize and automate services.** Partners emphasized the importance of creating more standardized processes, best practices, and tools. Failure to do so risks margins and profitability, particularly for partners servicing SMBs.

“The Microsoft team and comarketing funds have been beneficial. They help take away a lot of the new-deal complexity.”

Conclusion

FY 2024 was another year of solid deal-size growth with enterprise customers. For SMB customers, growth was significantly larger, including the second year of Multicloud Security and Compliance. Growth drivers included the rise of genAI and the need for companies to get AI-ready, the increasing complexity and frequency of cyberattacks, greater CFO scrutiny into why an IT organization is double-paying for security tools (when they have Microsoft 365 E5 or Microsoft 365 Business Premium), and Microsoft's continued investments that make it easier for partners to move into new security solution areas and go deeper with customers.

Managed services opportunities continued to grow as companies deal with shortages of IT and IT security professionals. This is especially acute in the SMB space, which helps account for the 53% increase in expected revenues for managed services. With regard to enterprise-customer managed services, this is the second year that Forrester has quantified the managed XDR services opportunity that partners have launched to tackle multivector threats and because of increased competition and maturity in the managed SOC and managed SIEM areas. Expected revenues for XDR managed services increased by 38%.

Partners expect this year's progress to continue and grow in FY 2025. This should be fueled by the genAI wave and by Microsoft's ongoing investment in security-related solutions and marketing. The partners applying the best practices described in this study are experiencing the biggest success, and this will continue to be the case in the years to come.

Summary Of The Microsoft Security Partner Opportunity (Enterprise)			
Solution area	Total revenue per user per month	Expected revenue per user per month	Expected YOY growth
Microsoft 365 Security	\$42.45	\$14.60	11%
Multicloud Security	\$23.45	\$9.00	10%
Compliance	\$20.35	\$6.70	16%
Identity	\$21.35	\$12.65	3%
XDR	\$11.65	\$2.35	34%
Total	\$119.25	\$45.30	10%

CONCLUSION

Summary Of The Microsoft Security Partner Opportunity (SMB)			
Partner Service	Total revenue per user per month	Expected revenue per user per month	Expected YOY growth
Microsoft 365 Security	\$39.20	\$14.30	17%
Multicloud Security	\$4.80	\$0.70	56%
Compliance	\$3.20	\$0.75	50%
Identity	\$4.90	\$1.95	11%
Total	\$52.10	\$17.10	19%

APPENDIX A: 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 Source: "The Partner Opportunity For Microsoft Modern Work," a commissioned study conducted by Forrester Consulting on behalf of Microsoft, July 2024.

³ 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, 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 Compliance and an MSSP will attach a lot more Microsoft 365. Use this calculation: total opportunity × attach rate = expected opportunity.

⁴ Source: [Security Survey, 2023](#).

⁵ Ibid.

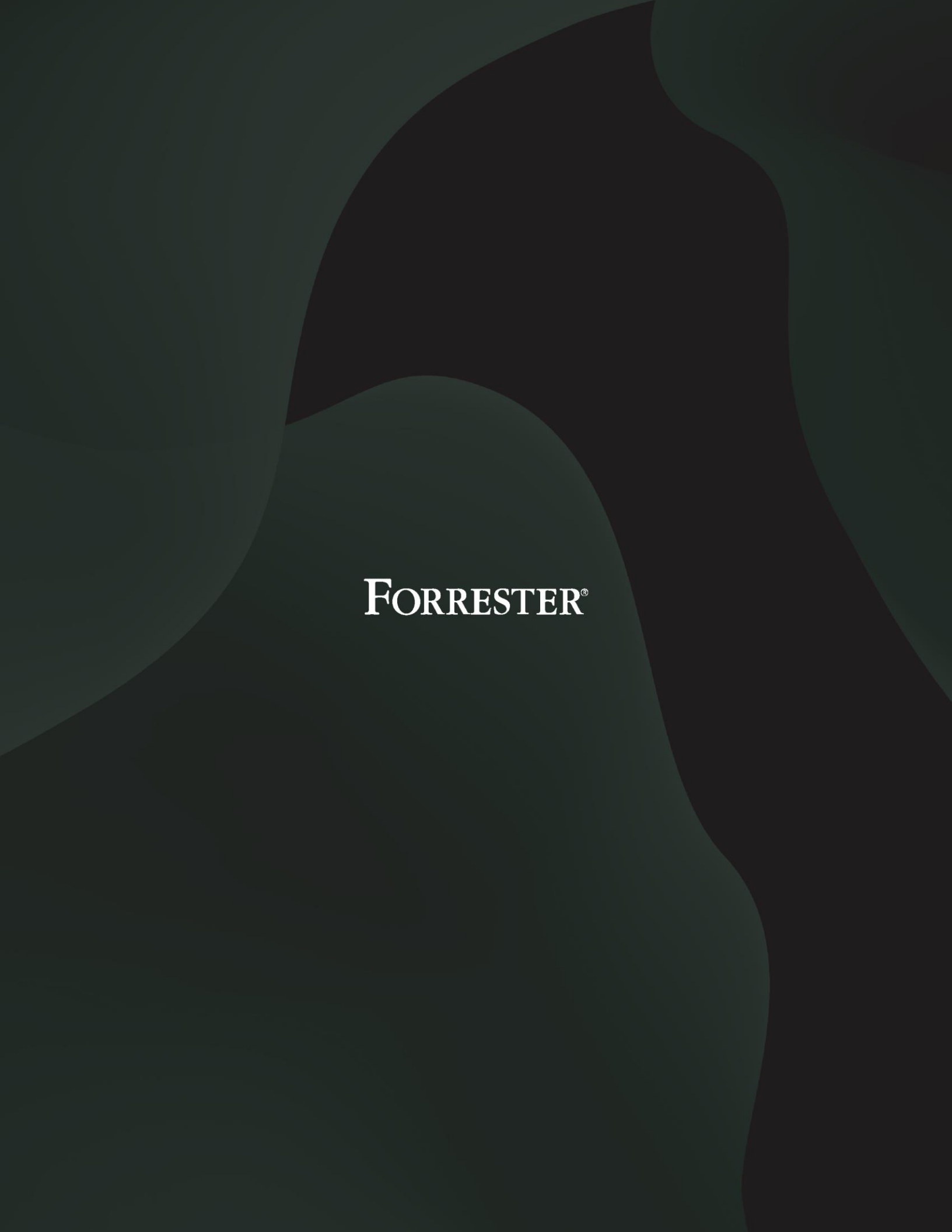
⁶ Source: [Global Tech Market Forecast, 2023 to 2027](#), Forrester Research, Inc., January 17, 2024.

⁷ Source: [Software 2 Survey, 2023](#).

⁸ Source: [Security Survey, 2023](#).

⁹ Ibid.

¹⁰ Ibid.



FORRESTER®