

# Disti

# Bootcamp

**Security momentum for SMB and sales engines**

Andres Garcia J

SMB Security Director

Microsoft Latinoamérica



# Security is top of mind for SMB customers

+300%

Ransomware attacks in the past year, with more than 50% targeted at small businesses <sup>1</sup>



1 in 4

Nearly one in four SMBs state that they had a security breach in the last year<sup>2</sup>

70%

Over 70% of SMBs think cyber threats are becoming more of a business risk<sup>2</sup>

90%

SMBs would consider hiring a new MSP if they offered the right cybersecurity solution<sup>2</sup>



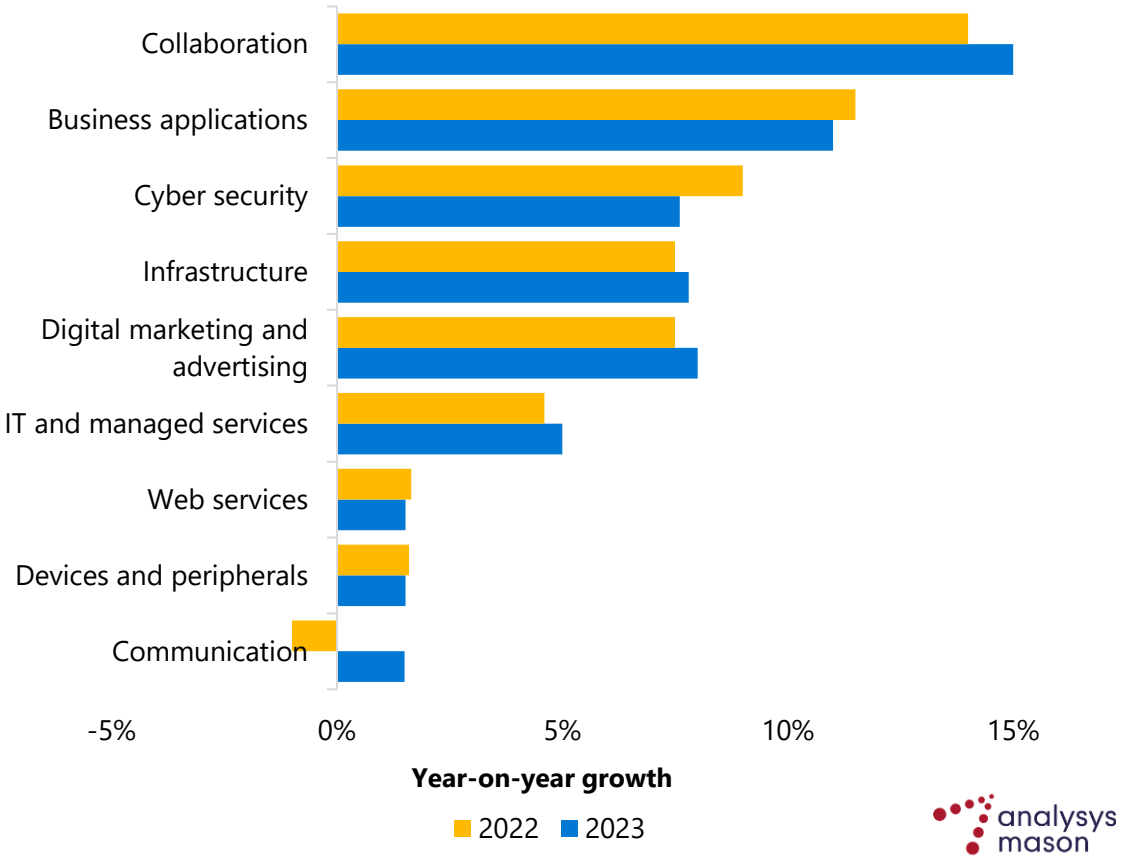
60%

of businesses close permanently within six months of an attack.<sup>3</sup>

1. [Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report](#)  
2. [Microsoft commissioned research, April 2022, US SMBs 1-300 employees](#)  
3. [Why small businesses are vulnerable to cyberattacks, May 2022](#)

# SMB market

YoY growth in SMB IT spending by solution category, worldwide, 2022 and 2023

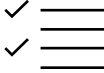


Source - [SMB IT spending 2022 by Anaysys Mason](#)

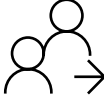
Source: Anaysys Mason



**Cybersecurity** is an ongoing concern for SMBs, especially with distributed and remote workforce.



SMBs will continue to spend on Security to prevent malicious attacks and **enhance business performance**.



The **relationship between SMBs and their channel partners is evolving** as SMBs seek support beyond IT purchases.

## SMB top of mind considerations for security solution



### Strengthen security

- Advanced security packaged for SMB
- Highly rated products, mobile security, endpoint security, network security



### Increase agility

- Scalability
- Easy to use and manage



### Gain efficiencies

- Cost-effective
- Pay as you go



### Vendor consolidation

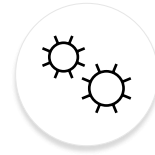
- Seamless integration
- Single vendor

# SMB customers security solution priority & decision influencers



## Top 5 Security Solutions<sup>1</sup>

- Network Security
- Mobile Security
- Endpoint Security
- Security Appliances<sup>2</sup>
- Web & Email Security



## Top 5 Buying Decision Influencers

- Product Effectiveness
- Price
- Brand Reputation
- Internet Research
- Online Review



## Why Purchase Through Vendor Online or MSP

- Trusted Advisor/Relationship
- Ease of Purchase
- Best Price
- Personal Relationship
- Corporate Account

<sup>1</sup> <https://www.analysismason.com/what-we-do/practices/research/smb-technology-forecaster/> –Year 2023 Data

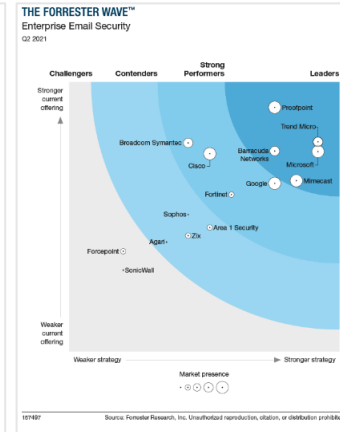
<sup>2</sup> Security Appliances - Network firewall and intrusion detection/prevention appliances)



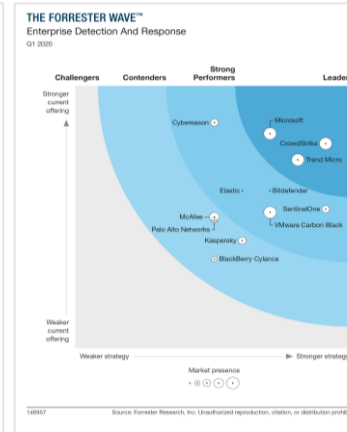
# Microsoft Security – a Leader in 9 Forrester Wave reports



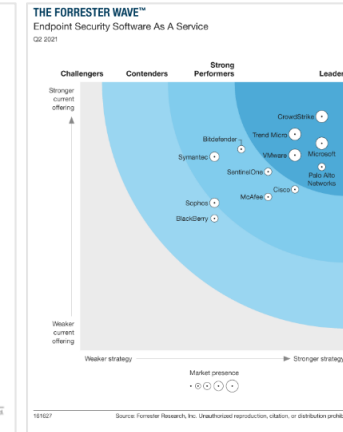
Security Analytics Platform



Enterprise Email Security



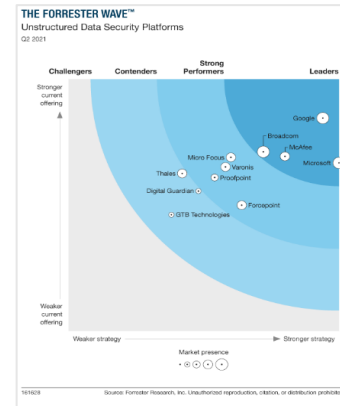
Enterprise Detection & Response



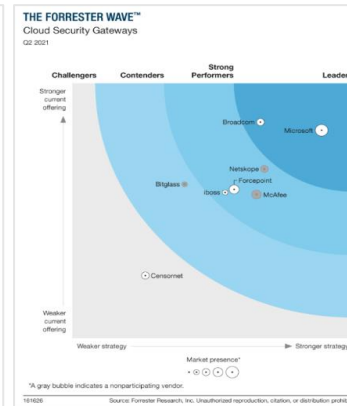
Endpoint Security Software as a Service



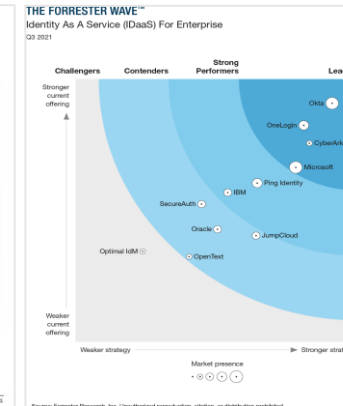
Unified Endpoint Management



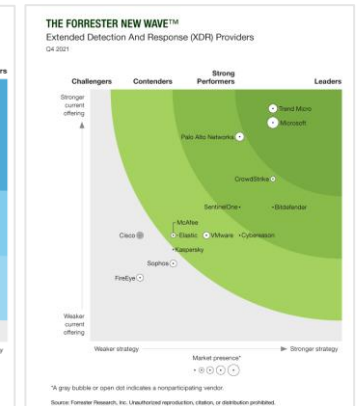
Unstructured Data Security Platforms



Cloud Security Gateways



Identity As a Service



Extended Detection And Response (XDR)

1. The Forrester Wave™: Security Analytics Platforms, Q4 2020, Joseph Blankenship, Claire O'Malley, December 2020
2. The Forrester Wave™: Enterprise Email Security Q2 2021 Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Enterprise Detection And Response, Q1 2020, Josh Zelonis, March 2020
4. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
5. The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, November 2019
6. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
7. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021
8. The Forrester Wave: Identity As A Service (IDaaS) For Enterprise, Q3 2021" by Sean Ryan, August 2021
9. The Forrester Wave™: Extended Detection And Response (XDR), Q4 2021, Allie Mellen, October 2021

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted™ using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



# Microsoft Security— a Leader in 5 Gartner Magic Quadrant reports



Access Management



Cloud Access Security Brokers



Enterprise Information Archiving



Endpoint Protection Platforms



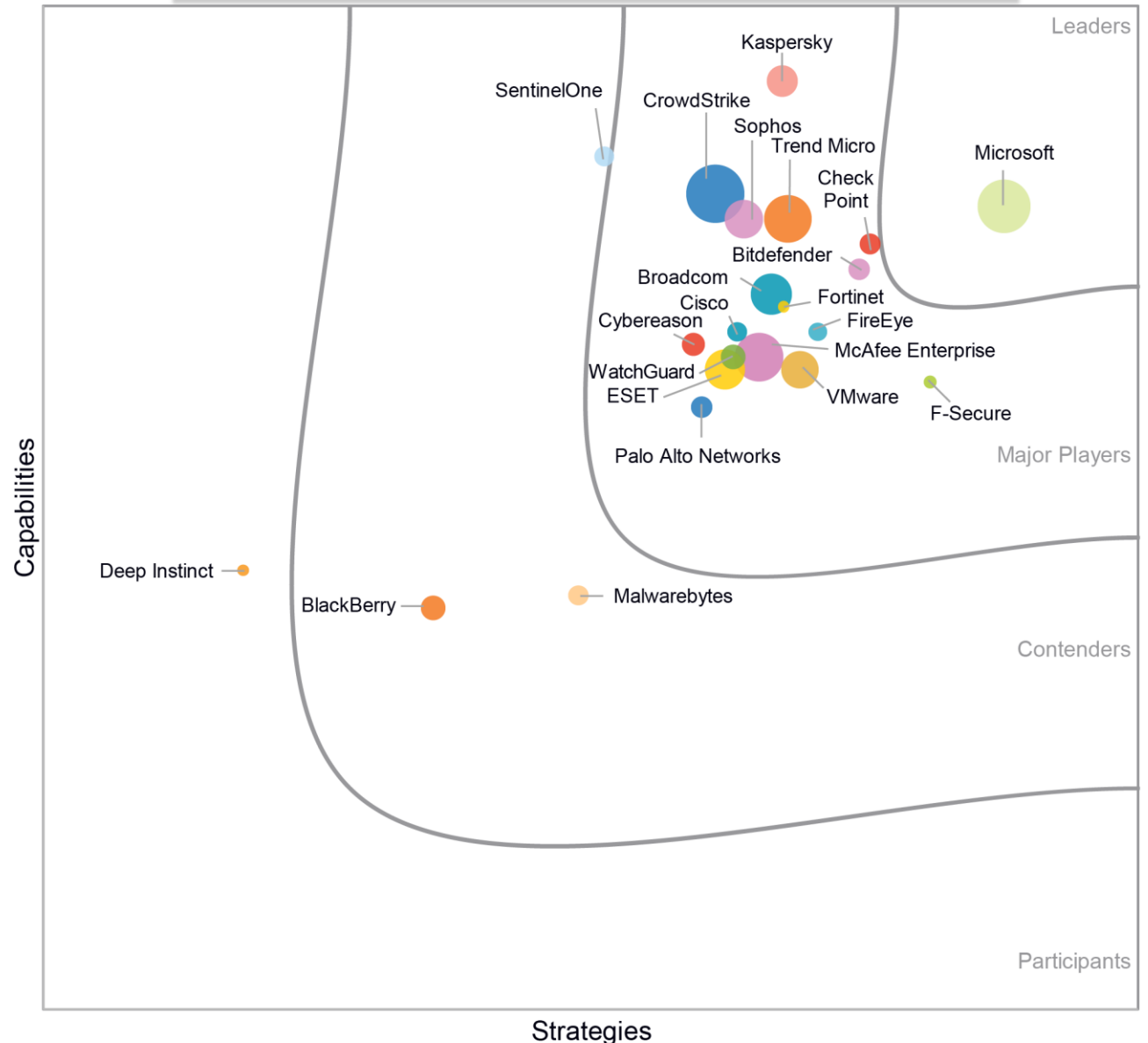
Unified Endpoint Management

- \*Gartner "Magic Quadrant for Access Management," by Henrique Teixeira, Abhyuday Data, Michael Kelley, November 2021
- \*Gartner "Magic Quadrant for Cloud Access Security Brokers," by Craig Lawson, Steve Riley, October 2020
- \*Gartner "Magic Quadrant for Enterprise Information Archiving," by Michael Hoech, Jeff Vogel, October 2020
- \*Gartner "Magic Quadrant for Endpoint Protection Platforms," by Paul Webber, Rob Smith, Prateek Bhajanka, Mark Harris, Peter Firstbrook, May 2021
- \*Gartner "Magic Quadrant for Unified Endpoint Management," by Dan Wilson, Chris Silva, Tom Cipolla, August 2021

*These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire documents. The Gartner documents are available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.*

# Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses

IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses, 2021



IDC MarketScape: Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment <https://idcdocserv.com/US48304721>  
 IDC MarketScape vendor analysis model is designed to provide an overview of the competitive fitness of information and communication technology (ICT) suppliers in a given market. The research methodology utilizes a rigorous scoring methodology based on both qualitative and quantitative criteria that results in a single graphical illustration of each vendor's position within a given market. The Capabilities score measures vendor product, go-to-market, and business execution in the short term. The Strategy score measures alignment of vendor strategies with customer requirements in a three to five-year timeframe. Vendor market share is represented by the size of the icons.

[Microsoft named a Leader in IDC MarketScape for Modern Endpoint Security for Enterprise and Small and Midsize Businesses - Microsoft Security Blog](#)

Source: IDC, 2021

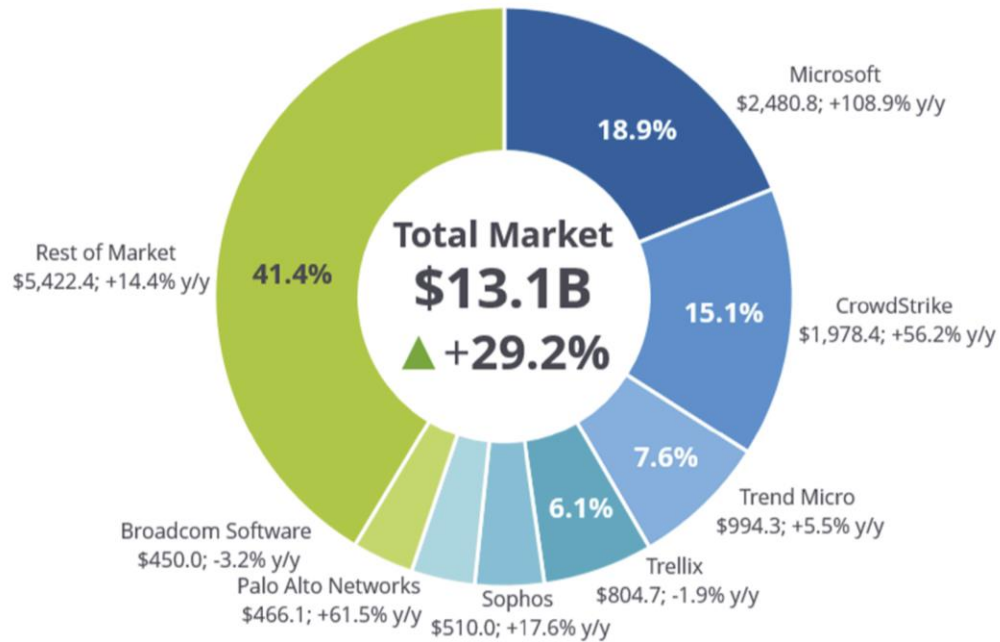


# Market Share leader in corporate endpoint security



IDC ranks Microsoft [#1 in WW Corporate Endpoint Security 2022 Market Share](#)

Worldwide Corporate Endpoint Security 2022 Share Snapshot

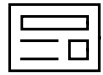


Note: 2022 Share (%), Revenue (\$M), and Growth (%)

Source: IDC, 2023

"...Microsoft has the highest market share at 18.9% in 2022 with a market share increase of 7.2 percentage points over 2021."

# Microsoft security solutions designed for SMBs



**Designed  
for SMB**

Advance security  
packaged for SMB



**Comprehensive**

Unlock employee  
productivity and  
accelerate digital  
transformation



**Gain  
efficiencies**

Scalable & cost  
effective



**Easy-to-use**

Easy to use and  
simplify security  
operations by  
Microsoft Partner



**Work securely  
from anywhere**

Secure remote work  
from anywhere and  
any device

# Microsoft SMB security offerings

## Microsoft 365 Security

**Microsoft 365 Business Premium<sup>1</sup> (<300 employee size customer)**

**Microsoft 365 E3<sup>1</sup>/E5 (>300 employee size customer)**

**Windows 365**

**Microsoft 365 Business Basic or Business Standard + Microsoft Defender for Business (<300 employee size customer)**

## Azure Security

**Microsoft Defender for Cloud<sup>1</sup>**

**Network Security – Azure DDoS IP Protection, and Azure Firewall Basic**

# FY24 Growth Aspirations | Security

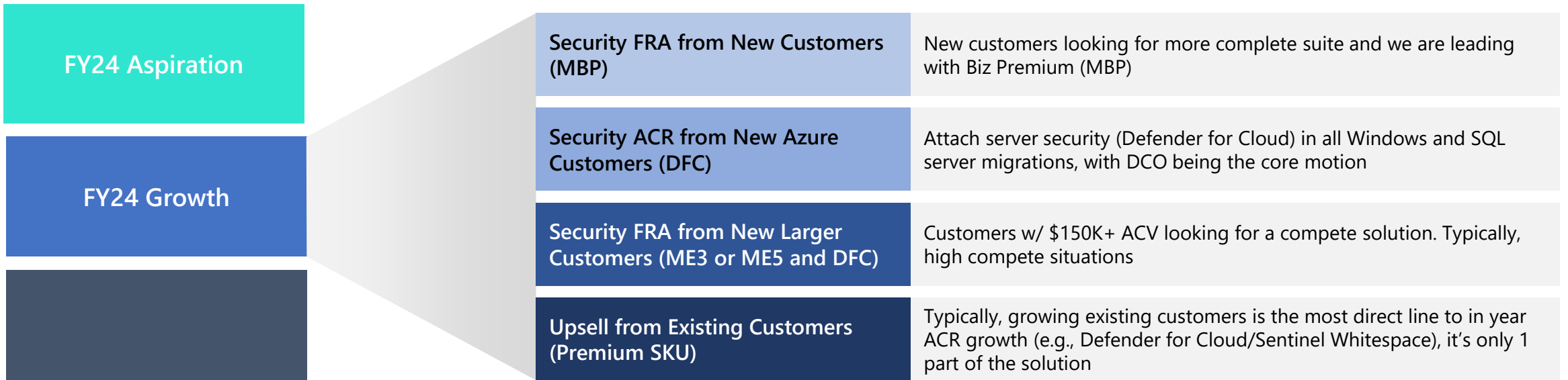


1

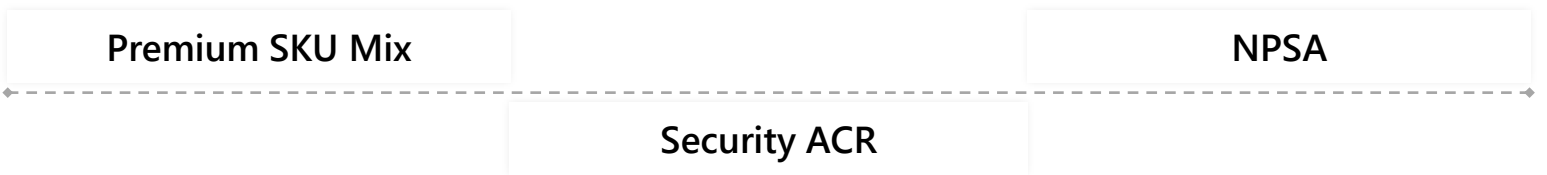
Objective

Security attach via core MW and AZ motions

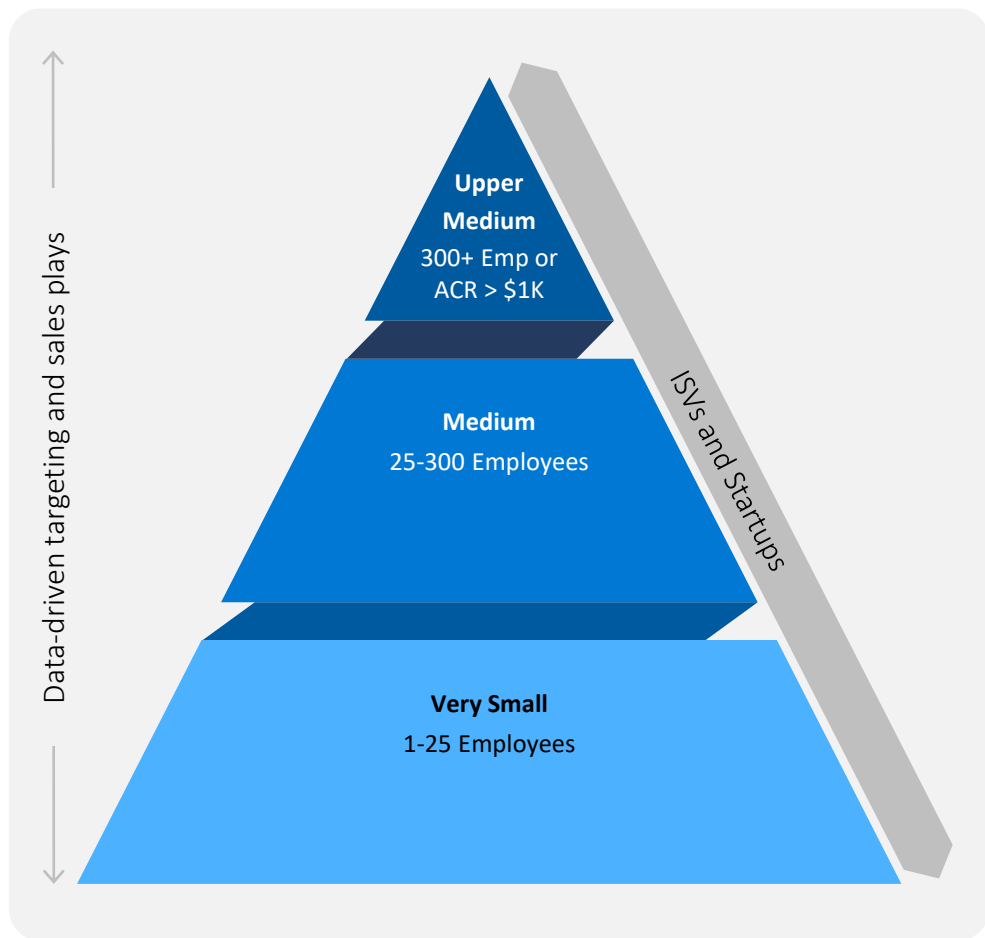
## 2 Growth Tactics



## 3 OKRs



# FY24 Latam SMB Segmentation



15M SMB Accounts  
\$27B TAM

## Upper Medium: ~30% Customer Penetration

TAM	Org Size	Accounts
\$8B	300+	50K

## Medium: < 10% Customer Penetration

TAM	Org Size	Accounts
\$9B	25-300	655K

## Very Small: < 5% Customer Penetration

TAM	Org Size	Accounts
\$10B	1-25	14M







# Addressing SMB customer's critical security scenarios

## SMB Business Need

## SMB Customer Scenario Example

## Why did this happen?

## How could this be avoided?

	 <b>Protect your Identity</b>	 <b>Protect Organization's Data</b>	 <b>Protect your Devices</b>	 <b>Protect Cloud Environment</b>
	<p>Identity-based attacks are becoming more sophisticated, forcing security teams to always be on the defense and protect their organization's data.</p> <p><b>For example, the CEO's, CFO's and other privileged identities has been stolen and used in fraudulent financial and data breach activities.</b></p>	<p>A breach of confidentiality that exposes sensitive information may be used for unfair advantage by a competitor or another person, which may have a detrimental effect on the company.</p> <p><b>For example, a data breach may occur when the release of a product specification occurs ahead of schedule or when personally identifiable information about customers is stolen.</b></p>	<p>Endpoint attacks have evolved significantly in the last 20 years, and as cybercriminals becoming more sophisticated very quickly.</p> <p><b>For example, when a user connects their infected personal mobile device to corporate network, the malware could spread through this connection and take control of the corporate resources</b></p>	<p>Vulnerability and misconfiguration of cloud resources can have an impact on an organization's operations, especially with the ever-present danger of cyber attackers.</p> <p><b>For example, a malicious actor could gain access to cloud resources, a DDoS attack could cause the website or application to go down, and users could be unable to access corporate data and applications.</b></p>
	<ul style="list-style-type: none"> <li>• Phishing and Spear phishing campaigns.</li> <li>• Credential stuffing.</li> <li>• Password spraying.</li> <li>• Man-in-the-Middle (MitM) attacks.</li> </ul>	<ul style="list-style-type: none"> <li>• Old and unpatched security vulnerabilities.</li> <li>• Malware.</li> <li>• Insider misuse.</li> <li>• Data leak.</li> </ul>	<ul style="list-style-type: none"> <li>• Ransomware, Malware, Exploits.</li> <li>• Vulnerability and misconfiguration.</li> <li>• Supply Chain Attacks (Solar winds).</li> <li>• Zero Day attacks.</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud Misconfiguration.</li> <li>• Lack of Visibility.</li> <li>• Malicious Insiders/Malware.</li> <li>• DDoS attacks.</li> <li>• Lack of Multi-factor Authentication.</li> </ul>
	<ul style="list-style-type: none"> <li>• Identity based Zero Trust Framework.</li> <li>• Implement MFA and go Passwordless.</li> </ul>	<ul style="list-style-type: none"> <li>• Simplify Access Permissions.</li> <li>• Encrypt All Data.</li> <li>• Implement a Data Leak Protection Solution.</li> <li>• Educate Staff.</li> <li>• Deploy Cloud Firewall.</li> </ul>	<ul style="list-style-type: none"> <li>• Endpoint security with Zero Trust framework.</li> <li>• Antivirus, EDR and XDR solutions.</li> <li>• Threat and Vulnerability with Automated Investigation and Remediation.</li> </ul>	<ul style="list-style-type: none"> <li>• Enhance security policies.</li> <li>• Use strong authentication like MFA.</li> <li>• Monitor and detect threats.</li> <li>• Turn on DDoS protection.</li> <li>• Deploy Cloud Firewall.</li> </ul>

# Security solutions addressing customers' business problems (1/2)

SMB Business Problem	Customer Scenario	Microsoft Security Solution	Key Customer Benefits
Multiple point solutions that increasing the operational costs, lack of integrated offering increasing reliability on support helpdesk and higher maintenance costs from multi-vendor licensing.	One solution that has all that customer needs to run and grow their business while having peace of mind that your business information is protected.	Microsoft Business Premium	Bring together comprehensive productivity tools such as Word, Excel, Outlook, Microsoft Teams etc. along with advanced remote access, security and device management capabilities.
With an increase in cyberattacks to SMB, threats are becoming more automated and indiscriminate, striking at a far greater rate.	SMB businesses need more protection from the top threats at a price they can afford.	Microsoft Defender for Business	Protect all the devices with the use of built-in automation and artificial intelligence to quickly identify and prevent threats.
Multi vendor productivity, and collaboration solutions without seamless security create additional costs and lack of operational efficiency challenges.	Customer wants to cut licensing cost and reduce deployment, and management costs, for e.g., patchwork.	Microsoft 365 E3	<ul style="list-style-type: none"> <li>• Improve productivity and foster a culture of collaboration with connected experiences.</li> <li>• Proactively protect employees, data, and customer information with intelligent security.</li> </ul>
Protecting the digital worker is more important than ever with the rise of remote work.	<ul style="list-style-type: none"> <li>• Temporary works (interns, contractors, vendors, etc.) who may need to access company data securely.</li> <li>• Data regulation requirements</li> <li>• Growth of third-party tools and disparate systems may leave vulnerabilities.</li> </ul>	Windows 365	<ul style="list-style-type: none"> <li>• Temporary workers can access company network/data securely and remotely from any device</li> <li>• Data, IP, and critical information is stored in the cloud, not locally on a device</li> <li>• Improve regulatory compliance via data centralization</li> </ul>



# Security solutions addressing customers business problems (2/2)

SMB Business Problem	Customer Scenario	Microsoft Security Solution	Key Customer Benefits
<p>Reduce business risk in the most effective approach. Have the right tool to protect the cloud workloads when things go sideways.</p>	<p>Customer running in Azure without security attack.</p>	<p>Microsoft Defender for Cloud</p>	<ul style="list-style-type: none"> <li>• Multi-cloud approach, single pane of glass across all platform with same security tool.</li> <li>• Risk reduction based on context, focus on what matter the most instead of getting lost in the noise.</li> <li>• Grow as you go, consumption model, lets you slowly expand and add coverage without multi-year large commit upfront.</li> </ul>
<p>Cyberattacks are increasing in volume and sophistication. More challenging to manage an expanding attack surface due to acceleration in digital transformation and shift to hybrid work.</p>	<p>Customer running in Azure without Firewall security or attach to current Azure customers planning migration.</p>	<p>Network Security – Azure Firewall Basic</p>	<ul style="list-style-type: none"> <li>• Cost-effective, enterprise-grade network firewall security</li> <li>• Easy to deploy and use</li> <li>• No maintenance (Firewall as a service model)</li> <li>• Seamless integration with Azure platform</li> </ul>
<p>DDoS attacks are rising in frequency and becoming more sophisticated. SMBs are highly targeted and often lack the budget and qualified staff to defend against DDoS attacks.</p>	<p>Customer running in Azure or planning to migrate to cloud needs protection of their resources from DDoS attacks.</p>	<p>Network Security – Azure DDoS IP Protection</p>	<ul style="list-style-type: none"> <li>• Cost-effective, enterprise-grade DDoS protection</li> <li>• Flexibility to enable protection on a single public IP</li> <li>• Seamless integration with Azure platform</li> </ul>

# Customer need translates to partner opportunity

85%

of partners see **security** as biggest area of growth<sup>1</sup>

How do we expand security services beyond basic AV?

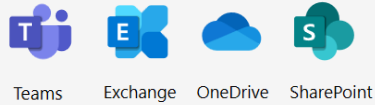
How do we deliver services at scale?

How do we do so without increasing cost?

# Microsoft 365 offerings for small & medium businesses

## Microsoft 365 Business Basic

### Cloud Services

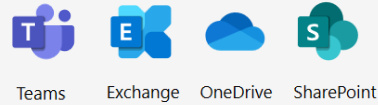


**\$6** per user/month

Formerly Office 365 Business Essentials

## Microsoft 365 Business Standard

### Cloud Services



### Desktop Apps

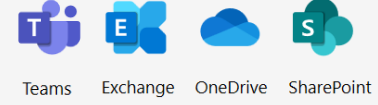


**\$12.50** per user/month

Formerly Office 365 Business Premium

## Microsoft 365 Business Premium

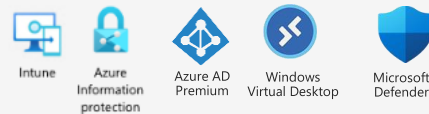
### Cloud Services



### Desktop Apps



### Comprehensive Security



**\$22** per user/month

Formerly Microsoft 365 Business

<sup>1</sup>price is subject to change based on subscription term, currency and region

Note: Not all features/product logos shown.

# CSP Incentives for Defender for Business and Microsoft 365 Business Premium

	Direct Bill Partner Incentives	Indirect Provider Incentives	Indirect Reseller Incentives
Standard Margin – 10-20%	✓	✓	✓
Incentives – 4% to 20%			
Modern Work & Security billed revenue	✓	✓	✓
Customer Add Accelerator			
Global Strategic Product Accelerator			

Partners can [apply here](#) to set up and run pre-sales SMB Workshops with potential customers to show them the value of Microsoft Defender for Business and Microsoft 365 Business Premium.

The CSP incentive program Product Addendum is the governing document detailing product applicability for each CSP incentive earning opportunity. Partners can access the Product Addendum on the [Microsoft Partner Website](#). <sup>1</sup>See FY22 incentive Guide for upcoming changes and supporting detail.

Classified as Microsoft Confidential and program information is subject to change. This asset is intended only for reference purposes, as a high-level overview of the program. Do not blog, tweet, post photos, or otherwise display information about this overview. Full details and program requirements are set forth and subject to the applicable program guide and partner agreement.

\*Local accelerators vary by region and SKU

# Announcing...

1 Acquire new customers and add users to existing customers

Get AI ready with  
Microsoft 365  
Business Premium  
promotion

15% off

for **NEW** Microsoft 365  
customers purchasing  
Microsoft 365 Business  
Premium in CSP

## Eligible markets

Africa

Korea

Canada

Latin America

Central and Eastern  
Europe

Middle East

Western Europe

France

Japan

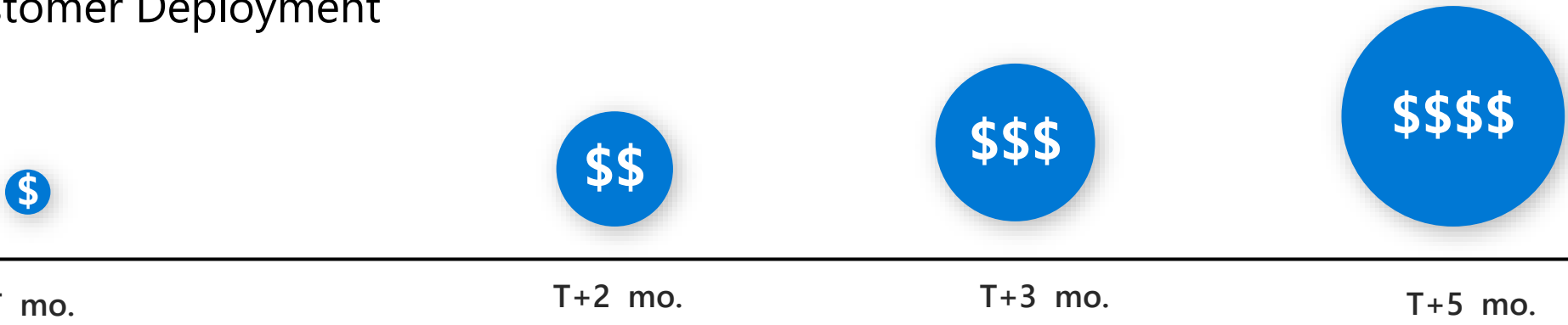
Review the FAQ for  
full country list

Available August 1 - December 31

For more details about the Microsoft 365 Business Premium New Customer Acquisition Offer in CSP, please review the <https://aka.ms/MWCSPPartnerFAQFY24H1>

# Create flywheel of ongoing managed services revenue with Microsoft 365 Business Premium

## Sample Customer Deployment



← Ongoing End user training and assessments →

Deliver value	Establish security baselines, deploy Teams, Office 365	Secure data	Get hybrid work ready Map to security standards	Optimize workflows
<b>Microsoft 365 Business Premium Features</b>	Office 365, Teams, MFA with Conditional Access Phishing/email protection with Defender for Office 365, Ransomware protection with Defender for Business Intune based device management Device provisioning with Autopilot	DLP /Azure Information Protection Cloud App Discovery	Full Microsoft 365 Business Premium security capabilities	Power apps
<b>Add-on services</b>	Migration and deployment Standardized identity and access security policies Endpoint security SOC/SIEM Device Lifecycle management	Data governance, retention and compliance policies e.g. Healthcare or Banking regulations Shadow IT Discovery and remediation	Implement full Security frameworks like NIST/CIS including recovery and remediation services Add-on Business Voice solutions Microsoft Teams Meeting Room solutions	Power Apps based workflows Azure Consumption Dynamics Upsell

# 2

## PLAN NUEVOS NEGOCIOS ADD ON

COMBINACIONES DE PRODUCTOS CON ELEMENTOS DE SEGURIDAD BUSINESS Y ENTERPRISE					
PLAN 1		PLAN 2		PLAN 7	
Microsoft 365 Business Basic	\$ 6,00	Microsoft 365 Business Standard	\$ 12,50	Office 365 E1	\$ 10,00
Defender for Office Plan 1	\$ 3,00	Defender for Office Plan 1	\$ 3,00	Defender for Office 365 P1	\$ 3,00
Defender for Business	\$ 3,00	Defender for Business	\$ 3,00	Defender for EndPoint P1	\$ 3,00
Total	\$ 12,00	Total	\$ 18,50	Total	\$ 16,00
PLAN 3		PLAN 4		PLAN 8	
Microsoft 365 Business Standard	\$ 12,50	Microsoft 365 Business Basic	\$ 6,00	Office 365 E1	\$ 10,00
Defender for Business	\$ 3,00	Defender for Business	\$ 3,00	Defender for Office 365 P1	\$ 3,00
Total	\$ 15,50	Total	\$ 9,00	Total	\$ 13,00
PLAN 5		PLAN 6		PLAN 9	
Microsoft 365 Business Basic	\$ 6,00	Microsoft 365 Business Standard	\$ 12,50	Office 365 E3	\$ 23,00
Defender for Office 365 P1	\$ 3,00	Defender for Office 365 P1	\$ 3,00	Defender for Office 365 P1	\$ 3,00
				Defender for EndPoint Plan 1	\$ 3,00
Total	\$ 9,00	Total	\$ 15,50	Total	\$ 29,00

# Start selling Microsoft Defender for Cloud



[Azure Foundations: Security & Defender for Cloud  
\(microsoft.com\)](https://microsoft.com)

## Tools to help you get started selling Microsoft Defender for Cloud

### Content in this workbook



**Conversation Guide:** Your sales team can use this guide to have meaningful conversations with your customers. Includes conversation starters, objection handling, and more!



**Solution-in-a-Box:** Find pricing tools and example components for Microsoft Defender for Cloud



# Microsoft Defender for Cloud Conversation Guide

## Conversation Starters

- How are you protecting servers running in the cloud?
- What security tools are you using to protect all your workloads, including cloud-based? What are the drawbacks?
- How are you storing your business data and customer information today?
- Are you able to connect all your servers, files, and data sources for security, visibility, and management?
- How much time do you estimate you spend identifying and responding to threats? How long does it take you to respond, on average?
- In what way has security management become more complex?
- Do you need to adhere to any corporate security policies or best practices? How do you ensure compliance?

## Overview and benefits of Microsoft Defender for Cloud security

Microsoft Defender for Cloud is a cloud security posture management and cloud workload protection that helps find weak spots across cloud configurations, strengthen overall security, and protect workloads across multicloud and hybrid environments from evolving threats.



**Protect across diverse workloads** whether on Azure, other clouds, or on-premises and meet regulatory compliance goals.



**Simplify security management** with a single portal that has built-in artificial intelligence and automation tools.



**Improve security best practices** through ongoing assessment, visualization, and recommendations.

## Objections and Responses

**Tip:** If customers are concerned about implementation complexity, this is an opportunity for you to offer managed services.

### *“Why do I need Microsoft Defender for Servers?”*

Microsoft Defender for Servers provides the tools you need to secure your servers across cloud and on-premise resources. It combines protection against external threats using a single solution for assessing your company’s security state. First, you can visualize how secure your servers with Secure score. Then you can strengthen your security with centrally managed policies and ongoing assessment and actionable insights.

### *“It sounds expensive.”*

Microsoft Defender for Cloud is a lot less expensive than you might think—and the costs of a breach can be extremely high. With two plans, you can choose the right protection for each server. And you may not need additional protection for some of them. I can work with you to determine how to right-size a solution specifically for you.

### *“My servers are already protected.”*

While many businesses think their servers are protected, sometimes these solutions are bolted on after the fact. I’d welcome the opportunity to work with you to ensure that you’re protected. One of the benefits of using Azure for security is that Microsoft uses a Zero-Trust model, which means “never trust, always verify.” That means that security is built in across all Azure services—and there’s not guessing on your part.

### *“This sounds too technically challenging.”*

Microsoft makes it easy to find the training you need to get started! You can get documentation, training, and resources on [azure.microsoft.com](https://azure.microsoft.com). **I can also work with you to get started.**

### *“What is the difference between Microsoft Defender for Endpoint and Microsoft Defender for Cloud?”*

We understand it can be confusing, because there is some overlap. Think about it this way: Microsoft Defender for Endpoint is dedicated to protecting devices like end-user PCs and phones, while Defender for Cloud protects all your infrastructure resources including servers running on-premises and in the cloud, as well as other cloud services—and that includes Azure and multiple other cloud platforms. Depending on plan, Microsoft Defender for Endpoint may be included in Microsoft Defender for Business, an endpoint security solution that helps businesses with up to 300 employees protect against cybersecurity threats.

# Microsoft Defender for Cloud

[Microsoft Defender for Cloud](#)



1. All costs are assumptions based on estimates from the Azure Pricing calculator and are not a guarantee of pricing for purchase. Prices may change based on region, working hours, and other variables. Because prices are subject to change, please use the Azure pricing calculator for your own estimate.

## Protect hybrid workloads with Azure security

Microsoft Defender for Cloud is an integrated solution designed to protect servers and other resources located anywhere. Start with Microsoft Defender for Servers to strengthen overall security, find configuration weak spots, and protect across on-premises, hybrid, and multicloud environments. Organizations can:

- Protect servers, data, and files, regardless of location
- Continuously assess security across on-premises, Azure, and other cloud scenarios.
- Protect against cyberattacks with Microsoft threat intelligence.
- Simplify security management with built-in controls and automation, plus AI for intelligent recommendations on next steps.
- Strengthen both security and regulatory compliance.

Pricing estimate for SMB customer infrastructure.<sup>1</sup>  
For latest pricing information [click here](#).

Defender for Servers can be added to a multicloud environment or existing Azure networking solution.				
Service type	Region	Description	Month	Estimated upfront cost
Defender for Servers plan 1		Gain advanced threat protection and management for cloud and on-premises servers.	\$4.90/Server/month	\$0.00
Defender for Servers plan 2		Includes all the features of plan 1 plus log analytics, security policy and regulatory compliance support, file integrity monitoring, and more.	\$14.60/Server/month Included data - 500 MB/day	\$0.00

For more details on plan features [click here](#).

## Deliver great value

Significantly improve your customer experience for less than \$20 per month. Microsoft Defender for Cloud is available at no cost for the first 30 days. After 30 days, purchase Defender for Servers with pay-as-you-go pricing.

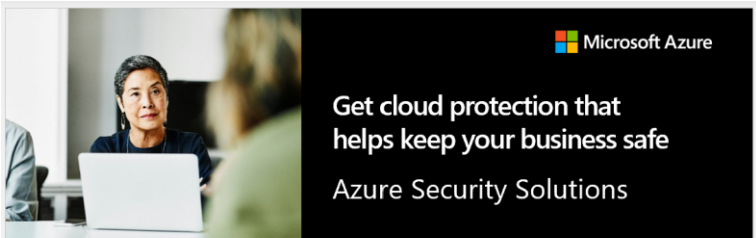
See the table below for estimated costs.

1. Check out pricing details for Defender for Cloud.
2. Register for the Pricing and Packaging webinar to help build an offering for your customers.

[Pricing details for Defender for Cloud](#)

[Azure Pricing and Packaging Webinar](#)

# Datasheet & Email Template



Get cloud protection that helps keep your business safe  
Azure Security Solutions

Small- and medium-sized companies are increasingly concerned about security. It's no surprise: the past year has seen a dramatic rise in remote work, which gives attackers more opportunities to damage data, networks, and identities.

#### Did you know?

**424%**

Increase in cyberattacks aimed at small businesses in 2020<sup>1</sup>

**\$149K**

The average cost of a data breach for a small- to medium-sized company.<sup>2</sup>

**43%**

Business that question whether they can identify and report a breach within 72 hours.<sup>3</sup>

## Advanced protection begins with Azure Security Solutions

When you choose Azure Security Solutions, you can start protecting your cloud and hybrid environments immediately, while setting the foundation for a solution that can be easily expanded.



### Improve security and compliance

Azure Security Solutions offer robust protection that helps secure your cloud and on-premises resources against malware, viruses, and DDoS attacks. You'll get the ability to continually assess how secure and compliant your business is—along with the ability to easily make adjustments and fix issues.



### Get protection across your business

With Azure Security Solutions, you can help safeguard all resources, whether they're servers, storage, databases, networks, applications, or firewalls. These solutions are all backed by Microsoft threat intelligence, so they work together seamlessly. And because they're Azure-native and highly scalable, you can easily extend services as you need them.



### Simplify security management

Azure Security Solutions make it simpler to manage security across your organization. You'll get a single portal, where you can centralize security policies and easily extend security to connected cloud resources. And advanced AI and automation are built in, so you can more quickly identify threats.

<sup>1</sup>Forrester, 3Q Surprising Small Business Cyber Security Statistics (2021)  
<sup>2</sup>IBM, 5.com, SMBs, Security Underestimated, Data Breach Costs  
<sup>3</sup>Infosecurity Magazine, GDPR is Stifling Innovation, Says Infosec Community

## Azure Security Solutions deliver next-generation security

Here's how to get started with Azure security:

### Microsoft Defender for Cloud

Understand your current security situation and get recommendations to improve it.

- A single portal to view and manage security and compliance
- A generated Secure Score to understand the security and health of your systems
- Detailed recommendations on how to improve your security

### Azure Firewall

A cloud-native, next generation firewall to protect your Azure Virtual Network resources.

- A scalable and highly available firewall-as-a-service
- Threat intelligence-based filtering with near real-time alerts
- Intrusion detection and prevention to continuously monitor and block malicious activities

### Azure DDoS Protection

Protect your applications from Distributed Denial of Service (DDoS) attacks.

- Turnkey defense for always-on traffic monitoring and automatic mitigation
- Adaptive tuning to learn application traffic patterns over time
- Multi-layered protection and detailed attack analytic reporting

## Put strong security foundations in place today

Security in the cloud requires security that's built for the cloud. That's where Azure Security Solutions can really help. Backed by Microsoft threat intelligence, you'll get robust protection that works across your entire infrastructure.

Getting started is simple. We recommend you begin with Defender for Cloud and go from there.



Let's do this together!

## Partner section with guidance

Note to partner—use this space to insert your own content, which can include customer testimonials, your qualifications to help them, calls to action ....

PARTNER LOGO

Microsoft Azure

Security breaches are on the rise.  
Are you protected?

More businesses than ever are running workloads in the cloud and in hybrid environments. At the same time, security threats keep growing and evolving. That means companies need robust protection that works as hard as they do.

Azure Security Solutions can help safeguard your business against threats, malware, network intrusion, DDoS attacks, and more. They work across all your resources, from databases to apps to networks. And because you can easily add services when you need, you'll get a great foundation that works today, and can grow as you need.

For more details, please check out the attached flyer. I'd like to chat with you more and answer any questions you might have. Please feel free to respond to this message or give me a call to schedule a time.

I'm looking forward to hearing from you!

Sincerely,

[Insert name and contact information]

This email and any offers it contained herein are brought to you by [Partner]

[Partner unsubscribe/privacy language]

[Partner postal address]

Microsoft provides this material for partners' convenience and informational purposes only. You may not change any of the claims made about Microsoft devices and services and must follow all Microsoft trademark guidelines. Consult with your own attorney to ensure you follow all applicable laws, including anti-spam laws.

#### Did you know?

The average cost of a data breach for small and medium companies is

**\$149,000.**

\*Forbes, 3Q Surprising Small Business Cyber

Azure security

# Quickstart guide

Protect hybrid cloud infrastructure against advanced threats with Microsoft Defender for Cloud.

## Partner Opportunity. Help customers:

- Protect servers, data, and files, regardless of location.
- Continuously assess security across on-premises, Azure, and other cloud scenarios.
- Protect against cyberattacks with Microsoft threat intelligence.
- Simplify security management with built-in controls and automation, plus AI for intelligent recommendations on next steps.
- Strengthen both security and regulatory compliance.

## Customer benefits:

Find weak spots across cloud configurations, strengthen overall security, and protect workloads across multicloud and hybrid environments from evolving threats.



**Protect across diverse workloads** whether on Azure, other clouds, or on-premises and meet regulatory compliance goals.



**Simplify security management** with a single portal that has built-in artificial intelligence and automation tools.



**Improve security best practices** through ongoing assessment, visualization, and recommendations.

## Learning tools: Learn how to help customers protect hybrid cloud.



### Interactive guide

Explore how to improve your Azure, hybrid, and multicloud environment.

[Get started](#)



### Guidance and best practices

Get an overview of Microsoft Defender for Cloud in Microsoft Docs, including guides and tutorials.

[Learn more](#)



### Video tutorial

Learn more about protecting multicloud environments.

[Watch](#)



### Introductory training course

Understand how Microsoft Defender for Cloud delivers protection and evaluate whether the solution is the right choice for your environment.

[Start course](#)

# SMB GTM Execution BOM: Packaged Sales Guidance

## 2, 1-pagers for CSA Solution Play Sales Journeys, aligned to MCEM

1

### Secure Productivity

Modern Work   Secure Productivity   Sales Journey					SMB
External facing	Listen & Consult	Inspire & Design	Empower & Achieve	Realize Value	Manage & Optimize
<b>Microsoft Outcome</b>	Solution Play confirmed & customer needs identified.	Solution Play value prop, channel and customer offers aligned to address customer need.	Solution Play executed through sales channel (Partner or Vendor/Tele) leveraging appropriate sales levers.	Solution delivered/employed. Sales channel (Partner or Vendor/Tele) supported with execution where needed.	Solution Play performance monitored & sales engine feedback provided.
<b>Partner Outcome</b>	Partner confirms Solution Play and/or partner solution is mapped against a customer need.	Partner has clarity on solution included in the deal.	Partner established in customer deal.	Customer satisfied with partner implementation.	Partner is able to grow their business.
<b>Hero Activities</b>	<p>Review <a href="#">Sales Execution Guidance</a> and select high propensity <a href="#">Secure Productivity</a> targets:</p> <ul style="list-style-type: none"> <li>Partner Cloud Ascent Data: <a href="#">Indirect Provider Overview &amp; Workbooks</a>, <a href="#">Cloud Ascent Partner Overview</a></li> <li><a href="#">Cohort Tool</a> – <a href="#">Coming Soon</a></li> </ul> <p>Review and leverage <a href="#">SMB Bill of Materials</a> to support discovery conversations and accelerate customer acquisition:</p> <ul style="list-style-type: none"> <li><a href="#">Coming Soon</a></li> </ul> <p>Access &amp; review Co-op funds resources including the Co-op guidebook:</p> <ul style="list-style-type: none"> <li><a href="#">Co-op Resources</a></li> <li><a href="#">Best Practices Resources</a></li> <li><a href="#">View available Co-op funds</a></li> </ul> <p>Equip partners with campaign-in-a-box materials to support marketing efforts:</p> <ul style="list-style-type: none"> <li>Execute an automated campaign via <a href="#">Digital Marketing Content OnDemand</a> (<a href="#">Coming Soon</a>)</li> <li>Leverage <a href="#">Partner Marketing Center</a> customizable assets (<a href="#">Coming Soon</a>)</li> </ul>	<p>Utilize SMB Workshops to demonstrate value, build customer intent, and accelerate opportunities for Modern Work and Security.</p> <ul style="list-style-type: none"> <li><a href="#">Partner SMB Workshops</a></li> </ul> <p>Initiate Solution Assessments to support customer comprehension of current technology environment and set the stage for next steps:</p> <ul style="list-style-type: none"> <li><a href="#">Solution Assessments</a></li> <li><a href="#">Partner Ready Resource</a></li> <li><a href="#">Modern Workplace Assessment Campaign Content</a></li> </ul> <p>Develop a business case based on your customer's specific needs using the Value Calculator and Training resources:</p> <ul style="list-style-type: none"> <li><a href="#">Value Calculator</a></li> <li><a href="#">Value Calculator Training</a></li> </ul> <p>Showcase Microsoft's proven solutions through relevant <a href="#">Customer Stories</a></p> <p>Leverage compete assets to get up to speed on the competition and understand key differentiators and talking points.</p> <ul style="list-style-type: none"> <li><a href="#">Modern Work Compete</a></li> <li><a href="#">Compete: Customer Leave-Behind</a></li> <li><a href="#">Microsoft 365 Partner Compete Guide</a></li> </ul> <p>Support your customer's AI roadmap utilizing <a href="#">AI Resources</a> and <a href="#">SMB AI Kit</a> to navigate AI conversations effectively</p>	<p>View below to access current/upcoming promotions.</p> <ul style="list-style-type: none"> <li><a href="#">Global Promo Readiness Guide</a></li> </ul> <p>Showcase Microsoft solution capabilities and benefits through <a href="#">Product Demos</a></p> <p>Drive customer confidence and smoother conversions through trial licenses.</p> <ul style="list-style-type: none"> <li><a href="#">Modern Work Trials</a></li> </ul>	<p>Use <a href="#">FastTrack for Microsoft 365</a> to help customers implement and go live so they can realize business value faster.</p> <ul style="list-style-type: none"> <li><a href="#">Microsoft 365 &amp; Security for Partners – FastTrack</a></li> </ul> <p>Explore resources and templates to help with managing adoption of Microsoft 365 in the <a href="#">FastTrack Resource Hub</a>.</p>	<p>Use <a href="#">Sales Advisor</a> to build and scale your customer lifecycle management (CLM) practice through data-driven decisions based on the health and interests of your customers.</p> <p>Enable earning opportunities for partners using Modern Work Partner Incentives. Refer to <a href="#">Incentives Guide</a> for details.</p> <ul style="list-style-type: none"> <li><a href="#">Channel Incentives: (MW/Security)</a></li> <li><a href="#">Partner Incentives</a></li> </ul> <p>Use the <a href="#">SMB Cohort Report</a> (<a href="#">Coming Q1</a>) to evaluate sprint performance and identify any potential gaps. Use the <a href="#">Cohort Tool</a> (<a href="#">Coming Soon</a>) to drive additional sprints to support gaps.</p>

Partner: [aka.ms/SMBMWSecureProductivityPartnerOnePager](https://aka.ms/SMBMWSecureProductivityPartnerOnePager)

2

### Migrate & Secure WS/SQL Server

Azure   Migrate & Secure Windows and SQL Server   Sales Journey					SMB
External facing	Listen & Consult	Inspire & Design	Empower & Achieve	Realize Value	Manage & Optimize
<b>Microsoft Outcome</b>	Solution Play confirmed & customer needs identified.	Solution Play value prop, channel and customer offers aligned to address customer need.	Solution Play executed through sales channel (Partner or Vendor/Tele) leveraging appropriate sales levers.	Solution delivered/employed. Sales channel (Partner or Vendor/Tele) supported with execution where needed.	Solution Play performance monitored & sales engine feedback provided.
<b>Partner Outcome</b>	Partner confirms Solution Play and/or partner solution is mapped against a customer need.	Partner has clarity on solution included in the deal.	Partner established in customer deal.	Customer satisfied with partner implementation.	Partner is able to grow their business.
<b>Hero Activities</b>	<p>Leverage the <a href="#">SMB SQL Migration Partner Sales Guide</a> for end-to-end guidance with all WS/SQL campaign execution partners, incl. campaign readiness &amp; SMB-specific scenario guidance.</p> <p>Review <a href="#">Sales Execution Guidance</a> &amp; select high propensity WS/SQL migration targets:</p> <ul style="list-style-type: none"> <li><a href="#">Sprint Tool</a> (<a href="#">coming soon</a>)</li> <li>Partner CLAS Data: <a href="#">Indirect Provider Workbooks</a>, <a href="#">Partner Center</a></li> </ul> <p>Drive customer demand:</p> <ul style="list-style-type: none"> <li>SMB-specific WS/SQL Campaign-in-a-box (<a href="#">coming Q1</a>)</li> <li>Utilize the <a href="#">WS/SQL Migration DMC</a></li> <li>For partners with Azure specialization, <a href="#">Migrate WS/SQL with AMMP</a> campaign</li> </ul> <p>Leverage SMB-specific Data Migration customer content: <a href="#">Outreach Mail</a>, <a href="#">Datashield</a></p> <p>Engage target customers with SMB-specific WS/SQL Migration value prop and drive customer next steps:</p> <ul style="list-style-type: none"> <li>SMB WS/SQL Pitch Deck (<a href="#">coming Q1</a>)</li> <li>SMB Data Migration Pitch Deck &amp; Telesales Guide</li> </ul> <p>Land Azure differentiated value prop with <a href="#">Achieve more with Azure</a> narrative.</p> <p>Embed security as a core component of WS/SQL migration motion with the <a href="#">SMB end-to-end security narrative</a>.</p>	<p>Utilize Partner-led <a href="#">SMB Reach for the Cloud</a> envisioning workshops to capture customer needs and confirm solution play requirements.</p> <p>Leverage Partner-led <a href="#">Azure Immersion Workshops (AIW)</a> for deep-dive <a href="#">Database</a> and <a href="#">Infrastructure</a> migration working sessions, including click-through demos.</p> <p>Utilize Solution Assessment to build customer cloud migration roadmap:</p> <ul style="list-style-type: none"> <li>Partner-led Assessment incl. Business Case w/ <a href="#">Azure Migrate</a></li> <li>Vendor Tele-led Evaluations</li> <li>Area Solution Assessment Desk for larger customer environments (<a href="#">Partner Nomination</a>)</li> <li>Scale Assessment Desk as single-entry point (<a href="#">coming Q2 FY24</a>) incl. partner requested Evaluations.</li> </ul> <p>For large, complex migration scenarios, leverage <a href="#">S2ARM</a> to align technical and/or Specialist resourcing support.</p>	<p>Deliver migration POC via Co-op utilizing <a href="#">Co-op Resources</a></p> <p>Lead with AMMP Partner-Led as primary CTA for customer migration projects (requires <a href="#">specialization</a>)</p> <p>If required for larger deployments, utilize <a href="#">AMMP Field-Led</a>, MSX opportunity &amp; nomination required.</p> <p>For near-zero code change rehosting scenarios, investigate <a href="#">Migration Factory</a> for no-cost migration services.</p> <ul style="list-style-type: none"> <li>Share <a href="#">customer/partner facing resources</a></li> <li>Submit <a href="#">nomination</a></li> </ul> <p>If required, leverage CSP ECIF &amp; ACO to win customer migration commitment to Azure, MSX opportunity &amp; nomination required.</p>	<p>Utilize <a href="#">FastTrack for Azure</a> to accelerate and de-risk migration deployments. <a href="#">Internal &amp; external nomination</a></p>	<p>Earn Azure CSP Consumption &amp; Workload Accelerator Incentives</p> <ul style="list-style-type: none"> <li><a href="#">Microsoft Commercial Partner Incentives Guide</a></li> <li><a href="#">Partner Investments &amp; Incentives – Internal</a></li> </ul> <p>Drive adoption of the Microsoft <a href="#">Well-Architected Framework</a> across customer &amp; reseller cohorts to improve workload quality and stability.</p> <p>Select additional WS/SQL footprint to migrate &amp; identify next Azure workload with <a href="#">CLAS</a></p> <p>Use the <a href="#">SMB Sprint Report</a> (<a href="#">coming Q1</a>) to evaluate sprint performance and identify any potential gaps. Use the <a href="#">Sprint Tool</a> to drive additional sprints to support gaps</p>

Partner: [aka.ms/SMBAzureMigrateWSSQLPartnerOnePager](https://aka.ms/SMBAzureMigrateWSSQLPartnerOnePager)

1-pagers for Security are the same Secure Productivity & Migrate & Secure WS/SQL Server

# Resources

**Grow partners sales and technical capabilities with CSP Masters Program**

[aka.ms/M365MastersProgram](https://aka.ms/M365MastersProgram)

**Grow acquisition and upsell with intent driven workshops and leverage on the new Business premium Promo (in select markets)**

[aka.ms/smbworkshoppartnerportal](https://aka.ms/smbworkshoppartnerportal)

[aka.ms/SMBPartnerPortal](https://aka.ms/SMBPartnerPortal)

**Partner Playbook/Kit**

[M365 Business Premium Partner Playbook](#)

[Defender for Business Partner Kit](#)

**Microsoft Defender for Cloud**

[Microsoft Defender for Cloud - CSPM & CWPP | Microsoft Azure](#)

[Azure Foundations: Security & Defender for Cloud \(microsoft.com\)](#)

# ¡Muchas gracias!

Andres Garcia

[andresg@microsoft.com](mailto:andresg@microsoft.com)

+ 57 3176484397

