



A PARTNER GUIDE

Build a security business that grows

Turn Microsoft security into revenue that comes back every month.

1 in 3

small and mid sized businesses were attacked in the past year.



What this guide covers

PART ONE

Why security sells

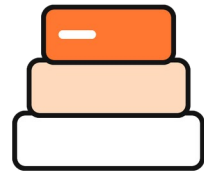
Who is getting attacked, what it costs them, and where the risk actually sits.



PART TWO

What to sell

Which licence to lead with, what to attach after it, and where your margin is.



PART THREE

Getting them to say yes

How to open the conversation, handle the pushback, and make the work come back.



Security is now part of every deal

Your customers are being pushed to adopt AI, keep customer data safe, and prove to an insurer that they are doing both. Whoever turns up with that conversation first usually wins it.



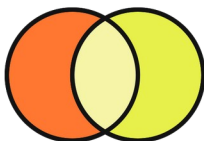
They own more than they use

Most customers already pay for security they have never switched on. Your first win costs them nothing new, and it buys you the second meeting.



The money comes back monthly

A licence renews once a year and you fight for it every time. Monitoring, reviews and reporting bill every month and renew quietly.



Almost nobody else is bothering

Under 300 seats is the segment most partners skip as too small to chase. Microsoft is actively funding the ones who do not.

PART ONE

Why security sells



Who is getting attacked, what it costs them, and the four places the risk hides in a small business.

Cybersecurity facts we cannot ignore

Each one answers a sentence you will hear in a first meeting, so you are not arguing from opinion.

1 in 3

were attacked in the past year, at an average cost of USD 254,000.

When they say they are too small

82%

of detections in 2025 involved no malware at all, up from 51% in 2020.

When they say they have antivirus

47%

of European small business owners are unsure how to protect the business.

When somebody doubts the demand

>99%

of unauthorised access attempts are blocked by multi factor authentication.

The very first thing to check

82%

of company data pasted into AI tools goes through personal, unmanaged accounts.

To open the Purview conversation

4x

year on year surge in shadow AI across organisations of every size.

To open AI governance

Sources: Microsoft Security research 2024, Microsoft Digital Defense Report 2025, Mastercard 2025, CrowdStrike Global Threat Report 2026, LayerX 2025, Verizon DBIR 2026.

Where the risk actually sits

Most customers protect email and assume the rest is covered. It is not. One question each is enough to find out.



Identity

Attackers now steal sign-in tokens, which gets them past passwords and basic MFA.

How do you find and fix risky access?



Endpoints

Work spans managed laptops and personal phones nobody controls.

How would you detect and contain it?



Email

Generative AI made a convincing phishing message cheap and scalable.

What happens after somebody clicks?



Data

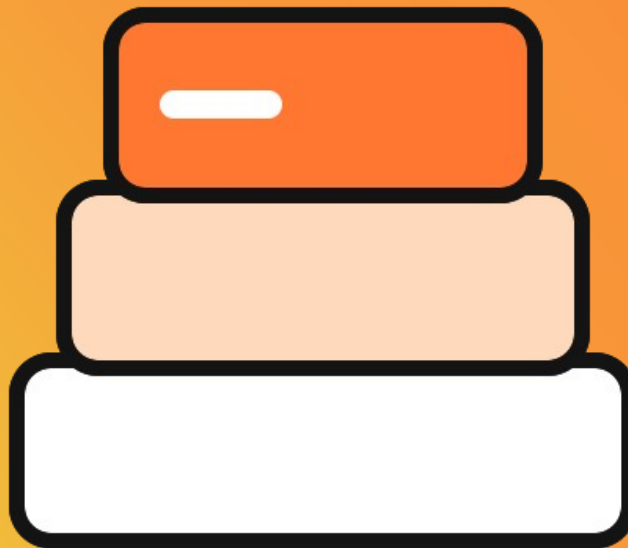
AI has increased the speed and reach of everyday data sharing.

Who controls what gets shared?

Ask all four and you walk out with an assessment, not a pitch.

PART TWO

What to sell



Land the foundation first, then attach the advanced suites once the risk justifies it.

What to sell, and in what order

Run your business securely is Microsoft's core security conversation for FY27, aimed at customers under 300 seats. These are the two key plays for the segment, and the ones Microsoft's FY27 promotions and partner funding reward most.

01

Secure the foundation

Microsoft 365 Business Premium

Identity, devices, email and apps covered in one place.

Your services: Assessment, migration, configuration, managed operations



02

Add advanced security

Defender Suite and Purview Suite

Stronger detection, data protection and governance, built for customers using AI.

Your services: Detection and response, data loss prevention (DLP), insider risk, audit, AI governance



Land first, attach second.

Selling both on day one is how the deal stalls. The foundation earns you the right to the second conversation.



What each step costs

On 1 July 2026 Business Basic and Standard went up in price. Business Premium did not. The suites are USD 10 each, or 15 for both, for up to 300 seats.

Business Premium

\$22

Copilot Basic, Entra ID P1, Intune P1, Defender for Business, Defender for Office P1

Defender Suite

+\$10

Entra ID P2, Defender for Endpoint P2, Office P2, Identity, Cloud Apps

Purview Suite

+\$10

Automatic labels, DLP across devices and AI, Insider Risk, eDiscovery. 50% off until 31 December 2026 when the customer also licenses Microsoft 365 Copilot Business or Microsoft 365 Copilot

Both suites

+\$15

Both suites under one subscription, up to 68 percent less than buying the same products as standalone licences

Microsoft 365 E5

\$60

The enterprise step, once a customer passes 300 seats



A comparable third party stack costs above \$43 per user. One platform cuts their annual spend by up to 23 percent, and that saving is what funds your services.

The business is the work around the licence

Somebody haggles over the licence at every annual renewal. The work you wrap around it bills every month, and that is the part the customer remembers.



Assess, configure, migrate, monitor, respond, govern and review are seven services you charge for. The licence makes them possible.

LAND	ATTACH	ATTACH
Business Premium • Security posture assessment • Identity and access management • Device management • Third party tool consolidation • Ongoing security management	Defender Suite • Advanced identity and access • Threat hunting and live response on endpoints • Email and collaboration security • Managed detection and response • Agentic AI security management	Purview Suite • Data loss prevention policies • Information protection and labelling • Insider risk management • Compliance, retention, eDiscovery • AI data governance advisory

Your customer gets up to 23% off their annual spend and up to 30% lower breach likelihood. You get a monthly invoice.

PART THREE

Getting them to say yes



Customers buy the answer to a question that has been quietly worrying them.

How to start the conversation

Ask one of these and then stop talking. Whatever they answer tells you what to propose, and in what order.

01

**If someone clicked a bad link,
how quickly would you know?**



02

**Who can open your sensitive
customer and financial files?**



03

**Has an auditor ever asked you
to prove how you protect data?**



Then let the findings do the talking.

The ALSO Security Assessment turns those answers into evidence, priorities and a next action.



What they say, and what you say back

“We already have another vendor”

Keep it for now. You are securing the layer underneath it: identity, devices and data. Compare the overlap when that contract comes up for renewal.

“Too expensive”

Add up what the current tools, the support contract and the admin hours actually cost, then compare that with one platform.

“We are too small to be a target”

One in three were attacked last year. Nobody picked them for their size, and antivirus does not cover identity, email, cloud apps or data.

“Our IT person handles it”

Then give that person one incident queue instead of five consoles, and something that responds at 2am when they are asleep.

“Ask us at renewal”

The renewal is decided months before the date on the contract. Run the assessment now, so your findings are what shapes it.

How one deal turns into a practice

The same five steps work on the tenth customer as on the first. That repetition is what turns a project into a business.

01

Look at who you already have

Find the customers with fragmented tools, thin protection, or a renewal coming up.

02

Find out what is actually broken

Review the environment together and agree which risks matter to the business.

03

Put a price on fixing it

Turn the findings into one recommendation, one number, and a plan they can say yes to.

04

Get it signed

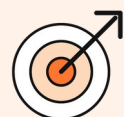
Agree the scope, who does what, when it happens, and what comes next.

05

Make it come back

Add monitoring, reporting and a regular review. Every review uncovers the next job.

**Book the first review
before the project closes.**



You do not have to build this alone

All three are available this week, so pick the one that matches where you are stuck.

01

Find the need

Run a security assessment on one customer and let the findings write your proposal for you.

[Security Assessment >](#)



02

Fill the pipeline

Ready made campaigns and assets, so you are not starting the conversation from a blank page.

[Growth Factories >](#)

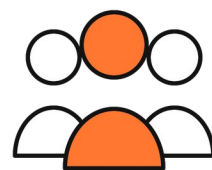


03

Build the practice

Training, specialist guidance and the programmes behind it, with people who have done it before.

[Elite Security Community >](#)





Start with one customer

[Book your Security Assessment >](#)

