PARTNER OPPORTUNITY PLAYBOOK

Securing Remote Work with Microsoft 365

Your guide to protecting SMBs from cyberthreats

CONTENTS

> … Groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails.[1]
>
> — Department of Homeland Security

Understanding the remote work challenge

Emerging risks for SMBs

Change is everywhere, from where, when, and how people work to the devices employees use to communicate, share, and access company data.

SMBs have played a key role in this dynamic business landscape. To successfully attract and retain talent—and quickly scale resources—many SMBs embraced a flexible workforce, offering greater opportunities to work from home and personalize hours. When COVID-19 emerged and most SMB customers had to rapidly shift operations offsite, remote work suddenly became the norm.

You've supported customers through this unprecedented time—keeping SMBs open for business while moving tons of data, once stored and accessed on-premises, to the cloud.

Now, SMBs face greater security threats as remote workers pose new risks. Customers that still rely on standard security measures, such as firewalls, antivirus, and backup solutions to keep their data safe, are particularly vulnerable to increased cyberattacks.

Why are SMBs at increased risk?

Employees working from home

Data being accessed from home PCs and personal devices

Increased phishing and ransomware threats due to shift to work from home

1. COVID-19 Exploited by Malicious Cyber Actors, Dept. of Homeland Security, April 2020.

A closer look

Why are SMBs vulnerable to security risks?

From a rapid rise in remote workers to a dynamic IT environment and an increasingly flexible workforce, your customers face greater security risks—both internally and externally—than ever.

58%
of breaches take place at small businesses

$120,000%
is the average cost for an SMB data breach

62%
of SMBs lack in-house security resources

It's little wonder that security is top of mind for SMBs. Reports show that 58% of breaches take place at small businesses,[2] resulting in a $120,000 average cost for an SMB data breach.[3] Meanwhile, 62% lack the skills in-house to deal with security issues.[4]

Businesses of every size have had to make a rapid shift to remote work due to the pandemic, and 70% of SMBs plan to maintain flexible work scenarios even after COVID-19 restrictions are lifted.[5] But, your customers face an even greater challenge now. They must address increased security risks while working to recover from the economic impact of the health crisis.

2. Verizon 2018 Data Breach Investigations Report. 3. Kaspersky Lab Study. 2018. 4. Underserved and Unprepared: The State of SMB Cyber Security in 2019. Vanson Bourne for Continuum.
5. Business Survey 2020: The Impact of COVID-19 on SMBs in the USA. Analysys Mason. June 2020.

What customers are saying

The impact of security threats on SMBs

When a data breach occurs at a Fortune 500 company, it can grab news headlines for days or weeks. Unfortunately, SMBs are even easier prey to hackers and other bad actors. And while attacks on them attract far less attention, your customers can suffer devastating results.

Hackers monitor companies for areas of vulnerability—often targeting smaller-sized businesses precisely because they know they have underinvested in security.

With cybercrimes increasingly more sophisticated, SMBs that lack advanced security tools and best practices face significant risks.

Here's what's happened to actual customers

> Someone was fooled by the email from the CEO and used his corporate card to send the iTunes gift cards. We lost about $5,000

— Adam A., video game rentals, 150 employees

> The only reason we caught it was that it was a 6-digit sales order and our sales orders are 7 digits."

— Joe B., food distribution, 250 employees

> We saw that it was moving through the network drives encrypting files, starting with Z: drive and moving down.

— Jerry K., import/export, 250 employees

> They got someone's password and sent an email to our CFO, who sent the $40,000 wire transfer.

— Bob K., property management, 150 employees

Understanding SMBs' security challenges

Meeting your customers' needs

Your customers face significant security risks with the shift to remote work, increased reliance on a flexible workforce, and greater numbers of devices (both company-owned and personal) used to access business data. You can help protect them from both internal and external threats by understanding their biggest challenges—and then providing the right solutions.

Lack of expertise

To address sophisticated cyberthreats

Not enough resources

To identify, assess, and mitigate security risks

Unfamiliar with security best practices

To prioritize best practices and educate employees

Too overwhelmed by solutions

To identify the right choice

With the growth in security threats, SMBs need help overcoming these gaps in expertise and resources. As a trusted partner, you understand your customers' current challenges. And you can help them identify and deploy the security solution that best fits their needs.

We created this playbook to support you—and help you win more customers.

3 ways to build a profitable practice

What's in it for SMB customers?

SMBs are concerned about security. In fact, nearly 90% of SMBs say they would consider hiring a new managed services provider (MSP) if they offered the right cybersecurity solution—and of those, 25% would be willing to pay more on average, too.[6]

That's why now is the right time to reach out to existing and potential customers. With Microsoft 365 Business Premium, you can provide SMBs with the security they need at a price they can afford, and even offer high-value services and expand your security practice.

Here's a closer look at the benefits to your customers:

Secure SMB customers

Meet pressing security needs with Microsoft 365 Business Premium

Reduce operational costs

Eliminate added costs for multiple third-party vendor solutions

Offer advanced services

Get affordable security with enterprise-level assessment and monitoring

6. The State of SMB Cyber Security in 2019. Vanson Bourne, commissioned by Continuum.

3 ways to build a profitable practice

What's in it for partners?

Building a thriving security practice for SMBs enables you to do more than help customers. It can also future-proof your business.

By selling Microsoft 365 Business Premium, you can boost your monthly profitability by $15.75 per user per month while offering customers a comprehensive security solution. And you can grow your security practice even more by providing high-value services and eventually fully managing your customers' outsourced security.

Microsoft 365 Business Premium can boost your profitability by $15.75 per user/month.

$720

Secure your customers

Sell Microsoft 365 Business Premium to current customers and reach new ones

- Licensing sales
- Base security features
- Supplement on-premises (Active Directory with Azure Active Directory)
- Reduce operational costs

+$310

Drive assessments

Add high-value, easy-to-sell services following deployment

- Cloud security assessment
- Hybrid security assessment (Cyber Security Assessment Tool)
- Compliance features implementation
- End-user security readiness

+$340

Monetize advanced service offerings

Grow the lifetime value of customer relationships with services that set you apart

- Monitoring and alerting
- IAM policy management
- Device policy management
- Threat remediation
- Compliance as a Service

Three-year average revenue per SMB seat from Microsoft 365 Business Premium

Source: The Microsoft 365 Partner Opportunity, A Forrester Total Economic Impact™ Study Commissioned By Microsoft, July 2019

Which product is right for your SMB customers

Microsoft 365 business solutions

Product names have changed, but you'll find the same value and price your customers want for Microsoft cloud productivity, desktop apps, and advanced security tools.

Specifically, Microsoft 365 Business Premium (formerly Microsoft 365 Business) gives your customers the cloud productivity tools they need to stay agile, with the built-in security and compliance tools SMBs require to keep their data safe—all conveniently available through the Microsoft Cloud Solution Provider (CSP) program.

Old product name		New product name
Office 365 Business Essentials	Cloud services	Microsoft 365 Business Basic
Office 365 Business Premium	Cloud services and desktop apps	Microsoft 365 Business Standard
Microsoft 365 Business	Cloud services, desktop apps, and advanced security	Microsoft 365 Business Premium

What's new?

Microsoft 365 Business Premium continually adds new features to better meet your customers' needs. Take a look at what's new and what it provides.

- **Conditional access:** Sets granular controls over who, when, and where business data is accessed
- **Multi-factor authentication:** Protects against unauthorized access
- **Self-service password writeback:** Simplifies password administration
- **Shared computer activation:** Supports multi-user or firstline worker scenarios
- **Windows Virtual Desktop:** Provides easy to manage virtualization that saves licensing costs
- **Enhanced Azure Active Directory access:** Enables secure remote access to work apps

Why partner with SYNNEX?

Get everything you need to build your security practice

When you resell with SYNNEX, you're partnering with a Fortune 500 company that continues to acquire and grow, despite challenging times. You can rely on our resources and expertise to make it easy for you to build the security practice that's right for your business.

Our team of subject-matter experts supports you every step of the way, so you can maximize profitable partner opportunities and deliver comprehensive security solutions to your customers. You'll gain direct access to all the services and support you need to win new business, like enablement funding to help you to close more deals and facilitate moving your customers to the cloud.

Another service you can leverage is DEMAND*Solv*, a free marketing solution for SYNNEX partners. With DEMAND*Solv*, you'll receive fresh marketing materials every week—which you can set on autopilot to send to customers and prospects, making your marketing effortless. Partners using DEMAND*Solv* report a **40% increase in sales and a 225% increase in sales leads**, while also improving relationships and engagement with both customers and prospects.

The SYNNEX difference

Our experienced team of subject matter experts provides the support you need to deliver comprehensive IT security solutions.

- **Assessments** – Our security assessments, complimentary vulnerability scans, penetration testing, and risk analyses will position you as a trusted advisor.
- **Pre- and post-sales support** – Leverage our pre-sales support services (including Microsoft engineer support, demos, implementation, and technical support) and post-sales support to help you succeed.
- **Training** – We'll provide you with ongoing technical training, including vendor-agnostic market overviews and vendor-specific product overviews for IoT and IT security.
- **White label IT security solutions** – Count on experts in security, networking, and unified communications to help you integrate security offerings with customers' existing solutions.

Check out Why SYNNEX + MSFT >

Why Microsoft 365 for remote work?

Built-in productivity, security, and compliance tools

Microsoft 365 Business Premium combines the cloud productivity tools SMB customers need, plus the advanced cybersecurity, device management, and data protection they require to stay secure and compliant.

As SMBs shift to a remote work model, employees need tools that empower them to collaborate and share documents, from anywhere, anytime. And productivity tools, such as video conferencing, chat, and cloud file storage, help your customers keep pace and pivot on a dime.

In addition, remote workers frequently use multiple devices, both company-owned and personal, to access data and stay productive. With Microsoft 365 Business Premium, your customers can easily manage every device across their organization with built-in security and compliance tools to keep data safe and deter threats.

Remote access and identity verification

Secure remote access and protect identity

Device protection

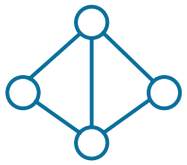
Secure personal and company-owned devices

Data protection

Safeguard confidential and business data

Securing remote access and identity

With the rapid rise of remote employees and the proliferation of a flexible workforce—from variable schedules and job sharing, to the use of contractors that help businesses scale up or down quickly—your customers need advanced tools that will keep their data and infrastructure safe. That's why Microsoft 365 Business Premium secures identity and controls remote access as people flex in and out of roles, regardless of where, when, and how they work.



Azure Active Directory

Controls who, when, and where workers connect to Office apps, protects against lost or stolen passwords with multi-factor authentication and conditional access, and enables employees to remotely access on-premises apps.

Windows Virtual Desktop

Securely enables remote desktop access, delivers a multi-session Windows 10 experience that is easy-to-deploy, cost-effective, and highly scalable, and supports any device platform including Windows, Android, Mac, iOS, and HTML5.

Advanced Threat Protection

Safeguards against malicious links, leverages AI-powered malware detection to scan attachments and shared documents, and uses Microsoft Defender Antivirus to protect Windows devices against suspicious processes such as ransomware.

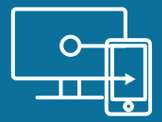
Since the start of the COVID-19 pandemic, WHO has seen a dramatic increase in the number of cyber attacks directed at its staff, and email scams targeting the public at large.

— World Health Organization[7]

7. WHO reports fivefold increase in cyber attacks. WHO. April 2020.

Protecting personal and company-owned devices

Employees today are just as likely to use personal devices as company-owned ones to stay productive, wherever and whenever they are working. To safeguard their data, your customers need an affordable solution that secures every device, regardless of who owns it. Microsoft 365 Business Premium provides advanced tools that make it easy to provision and manage devices across the organization.



Mobile device management with Intune

Manages access to all company-owned and personal devices, reports and measures compliance, provisions settings, manages access to email and files, and removes corporate data remotely.

Windows device management

Ensures automatic updates on all Windows 10 devices, enforces Microsoft Defender Antivirus protections against malware, and can require BitLocker encryption to prevent unauthorized access.

Windows Autopilot

Allows convenient drop-ship and automatic deployment of management-ready devices—including provisioning apps, configurations, and user settings for improved user experiences—and saves time and money.

Safeguarding confidential data

Increasing regulations and compliance requirements make it more critical than ever that your customers protect sensitive business and customer data. Yet, many companies worry that their own workers may employ shadow IT tools, which put them at risk. In fact, 57% of businesses say they feel vulnerable to losing confidential data[8] and 88% lack confidence that they would be able to detect or prevent the loss of it.[9]

You can keep your customers—and their confidential data—safe with Microsoft 365 Business Premium. SMBs can see exactly what's happening with their data and which tools their employees are using. As a result, your customers are confident they are compliant with regulations and their data is protected from internal and external threats.

Data loss prevention

Protects against accidental data leaks by identifying sensitive information across many locations and apps to prevent accidental sharing of data, and guides users to stay compliant

Azure Information Protection

Controls access to sensitive information, and provides restrictions and controls that stay with files and emails regardless of their location

Azure Cloud App Discovery

Provides visibility into cloud app use to understand shadow IT risk, record usage patterns, identify high-risk users, and bring applications under IT control

8. Insider Threat Report 2018. Veriato. 9. Security Concerns, Approaches and Technology Adoption. Forrester. December 2018.

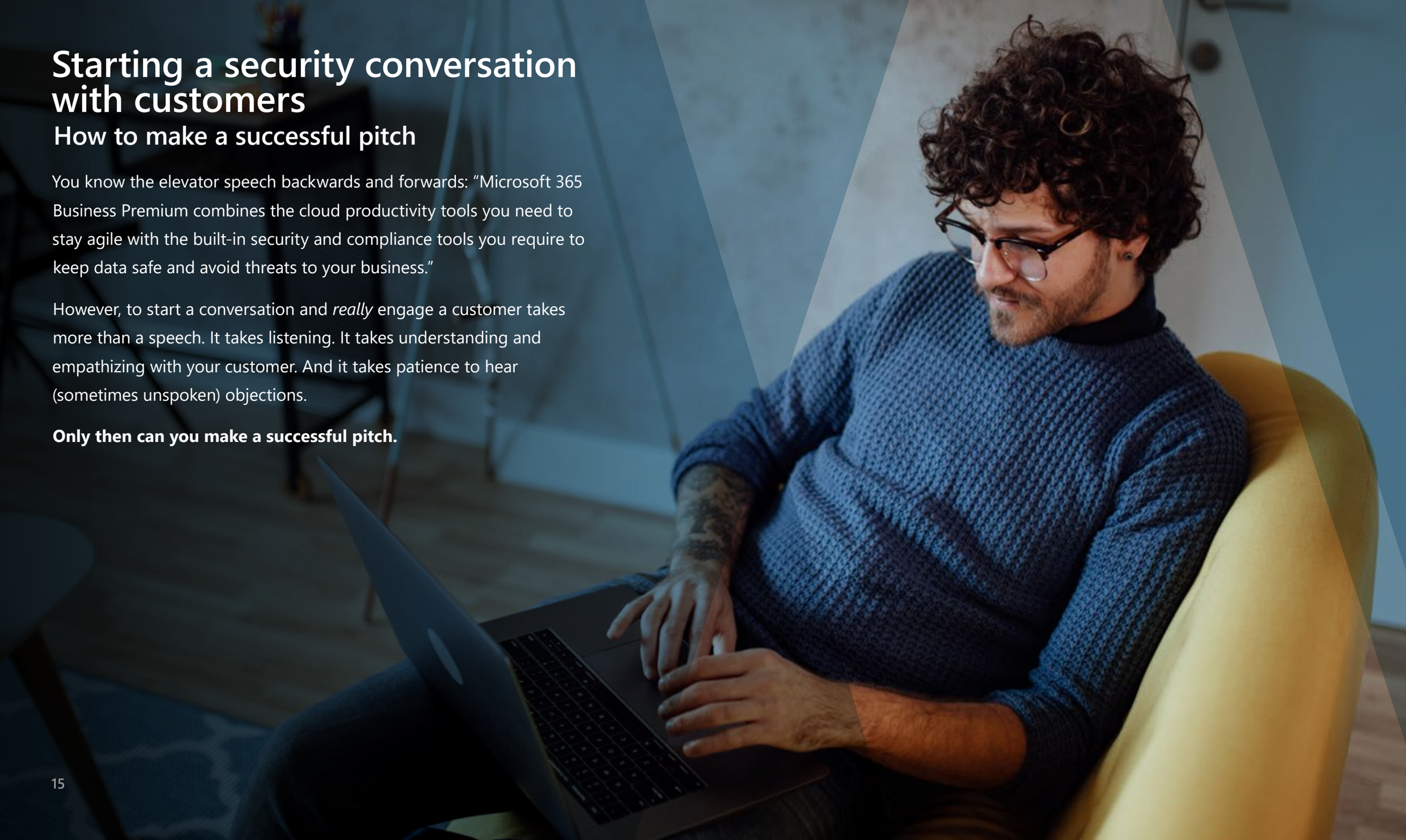
Starting a security conversation with customers

How to make a successful pitch

You know the elevator speech backwards and forwards: "Microsoft 365 Business Premium combines the cloud productivity tools you need to stay agile with the built-in security and compliance tools you require to keep data safe and avoid threats to your business."

However, to start a conversation and *really* engage a customer takes more than a speech. It takes listening. It takes understanding and empathizing with your customer. And it takes patience to hear (sometimes unspoken) objections.

Only then can you make a successful pitch.



Starting a security conversation with customers

Creating sales opportunities

Before beginning a conversation, start by identifying who your customer is, what opportunity they represent, and which type of event is the most compelling reason for them to improve their security. Then, when you're ready, choose a conversation opener.

Target audience (in order of prioritization)

1. An existing Microsoft 365 Business Standard (Office 365 Business Premium) customer
2. A customer considering Office 365 E3, currently using EM+S and/or third-party security solutions to converge investment
3. An SMB looking for the flexibility of the cloud, with increasing remote, flexible, or firstline workers
4. A customer with variable workforce scenarios and hardware requirements, looking to leverage employees' personal devices
5. An end-of-support Office and Windows customer

Customer opportunity

- One of millions of SMB customers ready to move to Microsoft 365 Business Premium
- The 50% of SMBs who would pay +20% more for the right security solution from a new MSP

Compelling event

- Dealing with work-from-home scenarios
- Responding to a security breach event
- Managing a flexible workforce
- Facing end of support for Office 2010 or Windows 7
- Anticipating device refresh and capital constraints
- Facing enhanced regulatory requirements (GDPR, HIPAA) in an industry or region

Conversation starters

- How do you ensure your data is not leaked, deleted, or accessed by someone who's not authorized?
- How are you protecting employees and your business from phishing attacks and ransomware?
- What steps do you currently take to keep employees' personal and company-owned devices secure?
- What would you do if an employee's device that contained confidential data was lost or stolen?

Overcoming objections

"Is Microsoft really a security provider?"

In one word: **Yes**.

Here's why. Microsoft delivers enterprise security for 90% of Fortune 500 companies.[10] That means it can offer SMBs unique insights informed by the analysis of 6.5 trillion threat signals daily and 5 billion threats detected on devices every month.[11]

Microsoft uses an AI-powered security graph that synthesizes data from a vast number of sources, connecting data points to draw a pattern that influences how other data points are interpreted.

In addition, Microsoft Defender analyzes signals and delivers real-time protection in milliseconds. As a result, your business is protected from software threats like viruses, malware, and spyware across email, apps, the cloud, and the web. And Microsoft Defender earned a perfect score from AV-TEST, an independent antivirus testing firm.

With over 3,500 people actively working on threat intelligence, Microsoft 365 Business Premium offers your business enterprise-grade, comprehensive security in a cost-effective package.

10, 11. Microsoft Internal Research.

Overcoming objections

"What if I'm not ready to move to the cloud?"

That's not a problem.

Microsoft 365 Business Premium is designed to work in the cloud and with on-premises resources, such as on-premises Active Directory, as well as security solutions from other vendors. So, you don't need to move to the cloud if you're not ready.

Of course, if you're still using Windows 7, it's worth considering the benefits of adopting Windows 10. First of all, it's the most secure Windows to date and it provides the best protection from threats. In addition, 99% of apps are Windows 10-compatible, which means that you can likely do an in-place upgrade.

Finally, if you already have devices that are licensed for a Pro version of Windows, Microsoft 365 Business Premium provides an upgrade benefit to Windows 10, which is a prerequisite for deploying Windows 10 Business.

Overcoming objections

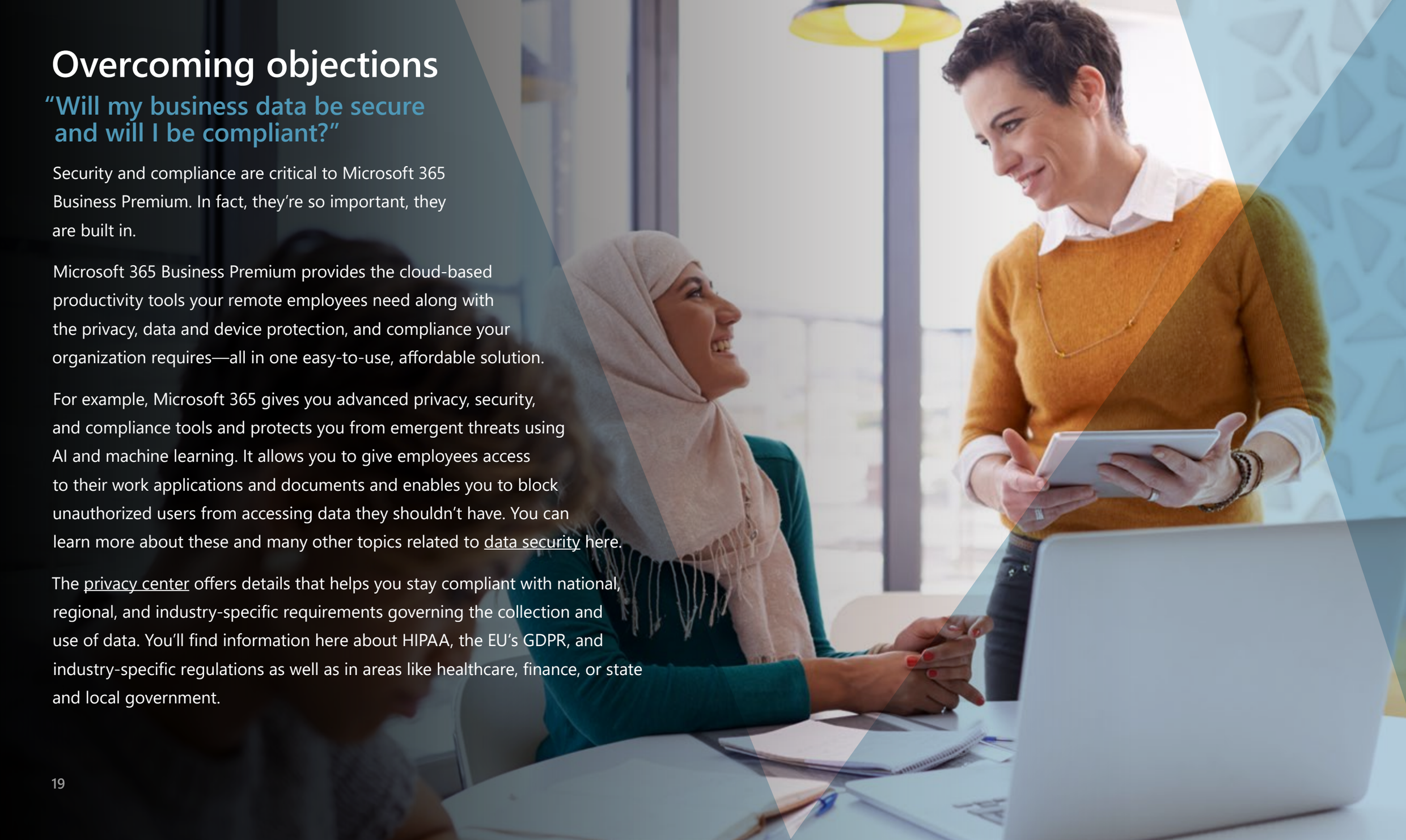
"Will my business data be secure and will I be compliant?"

Security and compliance are critical to Microsoft 365 Business Premium. In fact, they're so important, they are built in.

Microsoft 365 Business Premium provides the cloud-based productivity tools your remote employees need along with the privacy, data and device protection, and compliance your organization requires—all in one easy-to-use, affordable solution.

For example, Microsoft 365 gives you advanced privacy, security, and compliance tools and protects you from emergent threats using AI and machine learning. It allows you to give employees access to their work applications and documents and enables you to block unauthorized users from accessing data they shouldn't have. You can learn more about these and many other topics related to data security here.

The privacy center offers details that helps you stay compliant with national, regional, and industry-specific requirements governing the collection and use of data. You'll find information here about HIPAA, the EU's GDPR, and industry-specific regulations as well as in areas like healthcare, finance, or state and local government.



Overcoming objections

"I don't want another subscription, and I can't afford more security software."

I get it, but Microsoft 365 Business Premium can save you money over other solutions.

First, you get more value from a subscription-based cloud service like Microsoft 365 Business Premium than you do from locally installed software. You'll have the latest capabilities in productivity and security—for only $20 per user, per month. You'll have better support for your business growth and easier integration with other software and services. And, if you don't like it, just cancel the plan. It's that easy.

$12.50
for Microsoft 365 Business Standard

+

$7.50
for all these security features

- Advanced Threat Protection PI
- Intune
- Azure Active Directory Premium PI
- Azure Information Protection Premium PI
- Device Antivirus
- Autopilot
- Windows Virtual Desktop license
- Windows upgrade rights

=

$20.00
for Microsoft 365 Business Premium
(per user, per month)

Get started securing remote workers

Resources to protect SMBs

We have developed these curated resources to help you protect your SMB customers and secure their remote workers while building a profitable practice.

Use this list as a step-by-step guide to help you go to market, pitch and win customers, and drive higher recurring revenue for your business.

1 Learn how to secure your customers

Explore the Securing Remote Work Resource Hub
Get practical guidance on how to help customers secure their remote work environments, and access customer-ready go-to-market resources to drive the security conversation.

Watch the Webinar: Securing SMBs with Remote Workers
Learn how you can use Microsoft 365 Business Premium to secure remote and flexible workforces.

Learn to Deploy Remote Work Solutions
Need help providing customers with solutions for remote workers? Get the information you require.

2 Start the conversation with customers

Get the Go-to-Market Kit
Drive demand with an email series, start the conversation by customizing our pitch deck, and answer top customer concerns.

Showcase the Gaps with Secure Score
Get the visibility, insights, and guidance you need to show customers how to take full advantage of Microsoft 365 and Azure security.

Use the Return on Investment (ROI) Calculator
Use real customer data to show return on investment with Microsoft 365.

Use the Commercial Consulting Tool
Give your customer a tailored recommendation across key solution areas, like security and collaboration, and help evaluate their deployment readiness.

3 Dig deeper

Try the Microsoft 365 Business Premium Demo
Explore Microsoft 365 features with this hands-on demo.

Dive into Advanced Security for SMBs
Get curated resources and ready-made tools to build a profitable security practice.

Explore the Partner Growth Hub: SYNNEX + Microsoft
Learn how to grow a high-profit cloud practice with SYNNEX and Microsoft 365.

Let’s start boosting your business

Ready to help SMB customers protect their business while you maximize your margins? Check out the Microsoft 365 Securing Remote Work Resource Hub today.

Start offering Microsoft 365 Business Premium with SYNNEX. To get started, connect with our team at MSFTCSP@SYNNEX.COM.

GET STARTED >

SYNNEX brings the most relevant technology solutions to the IT and consumer electronics markets to help our partners sustainably grow their business. We distribute more than 30,000 technology products from more than 400 of the world’s leading and emerging manufacturers, and provide complete solutions to more than 20,000 resellers and retail customers in the U.S., Canada, and Japan.

SYNNEX CORPORATION