Microsoft

SMB Advanced Security Conversation Guide

Security is "providing access to information for those who need it and keeping out those who don't."

Microsoft 365 Business helps businesses defend against advanced cyberthreats and simplify IT management with a single solution.

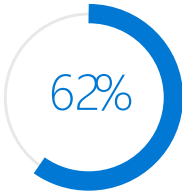
Help small and medium size businesses understand why they are most vulnerable.

Most of the headlines talking about cyber attacks are about big, well-known businesses. Yet small and medium size (SMB) organizations are especially vulnerable. Discounting this real threat can lead to inadequate security protections.

58% of breaches took place at small businesses.[1]

$120K

average cost of an SMB data breach.[2]



62% lack the skills in-house to deal with security issues.[3]

[1] Verizon 2018 Data Breach Investigations Report [2] Kapersky Lab study, 2018 [3] Underserved and Unprepared: The State of SMB Cyber Security in 2019, Vanson Bourne for Continuum

Probe for the biggest security pains

Email

Subpar antivirus antispam doesn't catch attacks

Users click on ransomware and phishing links

Users accidentally send confidential data

Mobility

Devices and laptops with company data can be lost or stolen

Inability to control who can access data

User credentials

Users have same passwords across all accounts, increasing risk if compromised

Attackers can easily steal credentials, then steal your money and take your files hostage

Compliance

Standards don't change based on company size

Requirements for GDPR and other regulations are rigorous and complex

Can they currently ...	Help them understand how Microsoft 365 Business helps ...
Defend against cyber threats?	• Protect email inboxes against spam and viruses • Block ransomware and phishing attacks • Configure advanced multi-factor authentication policies • Keep Windows 10 devices safe
Protect business data against leaks?	• Restrict copying and saving of business information • Block sharing of sensitive information like credit card numbers • Back up email in secure archive • Built-in mobile device management
Control who has access to information?	• Limit access to business information • Protect shared documents • Control business information on mobile devices • Strengthen secure access to devices
Secure mobile devices?	• Remote wipe of company data on lost or stolen devices • Require a PIN or fingerprint to access business documents and data to add an extra layer of protection
Prove compliance and risk mitigation?	• Runs on industry's most secure, compliant cloud with 24/7 support and financially backed SLAs • Built with enterprise-level protections that satisfy strict regulatory requirements • Automatic application updates • GDPR compliance with a private, secure, and compliant cloud

Overcome common objections

Common misconceptions that small and medium size businesses (SMBs) have about security contribute to the problem. Here are some ways to respond to common objections about the need for security.

Is Microsoft a security provider?

Microsoft has become one of the largest security providers in the world during the past few years, based on the myriad of threats it processes each day across more than 200 global cloud, consumer, and commercial services. Every month, Microsoft analyzes 400 billion emails in Outlook.com and Office 365 email services. More than 1 billion Azure user accounts provide insight into normal and abnormal authentications. Customers benefit from everything that Microsoft learns by defending against attacks and protecting identities.

We are a small business so we are not a target of any threats.

58% of breaches take place at small businesses. With an average cost per breach of $120,000, it's no wonder more SMBs are getting serious about security. Microsoft 365 Business provides the protection SMBs need with a comprehensive and trusted security solution to safeguard against threats to email, devices, and users.

Security is too complex and we don't have the staff to implement comprehensive security.

While SMBs may not have in-house IT departments, that doesn't mean they can't implement comprehensive security. Microsoft 365 Business provide one simple solution to deploy and manage; just activate protection capabilities as you would with other features. If your SMB customer wants more, you can offer advanced monitoring services using Microsoft tools.

Security is not a business priority for us.

SMBs that deal with customer information—whether they are retail, financial, health care, or food services—need enterprise-level protections. SMBs have the same accountability to secure data as big enterprises. Because Microsoft 365 Business has security built into the productivity platform, there is no need for trade-offs to justify the security investment.

What if I still have on-premises resources I need to access?

You can deploy Microsoft 365 Business for customers with on-premises Active Directory and local resources. You would configure the Windows device in one of two ways: Azure AD joined device or Hybrid Azure AD joined device. Learn more in this Tech Community blogpost.

Is my existing security technology compatible?

Microsoft has developed an open security strategy backed by the Microsoft Intelligent Security Association. Customers can take a layered approach to security and continue to use existing security solutions on top of Microsoft 365 Business. Optionally, Microsoft 365 Business can reduce maintenance and management costs by replacing multiple third-party vendor solutions.

Will I be able to comply with industry and government regulations?

Customers often find they get more value from subscription-based cloud services than from locally installed software. Benefits include apps purpose-built for small and medium size business, services that continuously enhance software and security, better support for business growth. If you don't like the service, just cancel the plan.

Drive home the value proposition

Defend against cyberthreats

Protect against phishing, ransomware, malware, and other advanced threats

Protect business data

Control who has access to sensitive information

Manage your devices

Manage the security of the devices that access your business information

How to win over customers:

1. Use an assessment to get your foot in the door

Evaluate how secure your customer's organization is and help define the desired state.

- Identify security objectives
- Assess current security state and identify security gaps
- Provide recommendations and best practices
- Create an actionable security roadmap

Cyber Security Assessment encompasses cloud and on-premises and is available from QS solutions. Or, customize an assessment using the free Microsoft assessment kit.

2. Share what customers say

"I'm no longer worried about security on the back end. I'm not worried about how secure our data is or even what third party apps we add. It's all taken care of through our Microsoft platform."

-Charles Sims
Head of Technology at Los Angeles Clippers

"We continually work to raise our Secure Score. Early on, the score feature was a driver in our choice to move to Microsoft 365—the better our security tools, the better we do our jobs, the better our security score."

-Justyn Bridge
IT Manager at Peet Limited

"Stade de France welcomes more than a million spectators a year, and we rely on the advanced security capabilities in Microsoft 365 as a critical part of our confidential data processing."

-Boulkerch Abdelkrim
IS Infrastructure and Production Manager at Stade de France