Microsoft

Advanced Security: Protect against cyberthreats

Deepen customer relationships and build recurring monthly revenue

Buyers

Primary: Owner/ CEO
Secondary:
Sales Directors
CFO
Business manager

Key customer concerns
- Preventing a costly data breach
- Improving the experience of distributed teams
- Protecting business and customer data
- Staying compliant
- Getting more value from your money
- Minimizing the number of security products from multiple vendors

Solution value

Microsoft 365 Business combines Office 365 productivity tools with a comprehensive security solution that protects your business against advanced cyberthreats.
- Help protect against sophisticated threats hidden in online email attachments and links – ATP Safe Links.
- Protect against sophisticated malware with analysis of email attachments – ATP Safe Attachments
- Anti-phishing policies – ATP anti-phishing intelligence
- Configure advanced multi-factor authentication policies – Azure MFA – Trusted IPs
- Enforce malware protection across Windows 10 devices – Windows Defender
- Protect sensitive data from leaking – Data Loss Prevention
- Encrypt email for recipient-use only – Message Encryption
- Label and set permissions for files to ensure confidentiality – Azure Information Protection.
- Control which devices and users can access data – Conditional Access
- Apply policies to protect data on phones – Intune MDM
- Keep business data inside approved Office mobile apps – App protection for Office mobile apps
- Remotely wipe company data from lost or stolen devices – Selective Wipe from Intune.

Differentiator
Powered by the Microsoft Intelligent Security Graph, Microsoft 365 offers unique intelligence plus a complete approach to security. Advanced features help you give customers the visibility they need to take action plus helps you demonstrate your value.

Customer value scenarios

Defend against threats- Help protect against malware, viruses, phishing attempts, malicious links, and other threats

- Check links at click to combat advanced phishing
- Detect malware with sandbox analysis of email attachments
- Enable anti-phishing policies that use ML
- Enable advanced multi-factor authentication
- Enforce features to protect Windows 10 devices

Protect business data-Help keep personal and financial information safe. Make it easy to maintain customer loyalty and comply with industry regulations.

- Encrypt sensitive emails
- Block sharing of sensitive information like credit card numbers
- Restrict copying and saving of business information
- Enable unlimited cloud archiving

Secure devices-Help customers embrace mobile productivity without worrying about security exposure.

- Control which devices and users can access business information
- Apply security policies to protect data on iOS and Android devices
- Keep company data within approved apps on mobile devices
- Remove business data from lost or stolen devices with selective wipe

Building your offer

Offer	Description	Compelling Events
Microsoft 365 Business	Built-in security capabilities that seamlessly protect user's identity, devices, documents, and emails with encryption and access control based on policies set by your IT team	Security breach event
		End of support for: Office 2010, Windows 7
		Regulatory requirements such as GDPR

Protect your organization against external threats

Target

1. Highest propensity customers are ones using Office 365 Business Premium in your base. Prioritize these first.

2. Small and medium size customers considering Office 365 E3 are also high propensity due to higher security functionality in Microsoft 365 Business.

3. Next priority are customers with third-party security point solutions to provide them baseline security across vectors.

4. Use **compelling moments** as a reason to approach them (SecureScore analysis, a recent security breach event, device refresh, new regulatory requirements such as GDPR).

5. Understand concerns owners have with security and ensure that you address them in your pitch.

Discovery questions:
- Have you had any recent security incidents you are aware of?
- What are your security concerns?
- Can you quickly identify suspicious activities and attacks?
- How do you secure platforms and devices, especially for mobile or remote workers?
- How do you maintain visibility and control, and protect applications?

Use marketing and engagement assets for each customer stage

LEARN	MARKET	SELL	DEPLOY
Product technical readiness	Partner resources	Partner resources	Microsoft 365 Deployment Kit
SMB guided product tour	Offer builder	Partner Smart Office and SecureScore	Adoption resources
Demo platform	Cyber Security Assessment Tool (CSAT) from QS Solutions		
Certification			

Best practices

- Educate yourself about Microsoft 365 security capabilities and review the Microsoft commitment to security and compliance.
- Use marketing and engagement assets for each sales stage.
- Build and present an **example offer** using the Offer builder tool.
- Use assessments with customers to help them think through capabilities and land deals.
- Offer customer education on key scenarios, such as setting up MFA, email best practices and MDM
- Engage the right team, including the **top influencers** who need to be persuaded that the cloud can be more secure than an on-premises server.
- Show the overall value – the cost for Microsoft 365 Business is often less than the standalone cost of the security components needed. Alternatively, Microsoft 365 features add more layers of protection working with third-party products from Microsoft security partners
- Discuss **managed services** and **advanced offerings** based on customer needs. Emphasize included reporting that helps justify business value.

"We don't wait for customers to talk about security, we lead with it as something that's critical. We don't use fear-mongering, though. Our approach is to ask 'Have you thought about these things? Here's what could happen, and our recommendation."   - Jason Fox, Software architect, Rackspace

How to tailor the conversation

Situation	Focus on helping the top executives understand…
Financial Services	Microsoft has information protection and data loss prevention capabilities that help prevent sensitive financial and customer data from leaking.
Healthcare	Microsoft has information protection and data loss prevention capabilities that help prevent sensitive financial and patient data from leaking.
Retail	The cloud can provide better security than many retailers can provide with on-premises solutions. Data protection capabilities can help protect customer data.