How Microsoft 365 Business can help secure your organization
Table of contents

01  Microsoft 365 Business: the security solution for your business
02  Help protect data across devices, both personal and company-owned
03  Classify data and help prevent accidental leaks
04  Help protect your users from external threats
05  Have peace of mind that you’ve got access to your data
01.

Microsoft 365 Business: the security solution for your business
It’s difficult to run a business today without thinking about security. Almost every day you hear or read about new threats and vulnerabilities, from the latest malware to yet another data breach. Whatever your business is—large or small, a few customers or millions, one device or hundreds—you need to keep threats from compromising your data, your devices, and your ability to run your organization.

Security is hard, however, because there are so many moving parts, which means that safeguarding your company can be expensive, difficult, and time consuming. Microsoft 365 Business gives you peace of mind by protecting your business in an integrated, simplified way. With just a single subscription, Microsoft 365 Business gives you a layered approach to security that helps:

- **Protect** your business from threats, especially external cyber attacks
- **Safeguard** company data across devices and apps
- **Prevent** intentional and unintentional data leaks
- **Preserve** data so you can access it anytime, including for compliance reasons

The enterprise-grade security provided by Microsoft 365 business can help support your organization at every stage of your growth and transformation. In this e-book, we’ll show you some of the most useful security features in Microsoft 365 Business and explain how they help protect your organization.
02.

Help protect data across devices, both personal and company-owned
Microsoft 365 Business gives your employees the flexibility to work on PCs, Macs, phones, and tablets, even in browsers—whether on a personal or company-owned device. If a device is ever lost or stolen, you can still prevent it from accessing, retaining, or sharing business information.

Microsoft 365 Business handles mobile device management (MDM) and mobile app management (MAM), securely managing your organization’s mobile devices and apps, including iOS and Android devices. In addition, with Microsoft 365 Business, you can also use the selective wipe feature, which removes business information from an employee-owned device while leaving their personal information intact.

How Microsoft 365 Business helps keep your business secure

- Gives you peace of mind by allowing you to remotely wipe business data on lost or stolen devices without affecting personal information
- Helps you issue company-owned devices and support a bring-your-own-device (BYOD) program
- Helps protect all your email and data so that they can be accessed by mobile devices
- Allows you to provide limited-use shared tablets to your task workers
03. Classify data and help prevent accidental leaks
How do you control and secure email, documents, and sensitive data that you share outside your company walls?

And what if your organization faces regulatory requirements for protecting sensitive information and preventing unauthorized disclosure? For example, maybe you’re required to secure financial data or personally identifiable information (PII), such as credit card numbers, social security numbers, or health records.

Microsoft 365 Business gives you data protection at all times, no matter where the data is stored or who it’s shared with.
Here’s how it works

Microsoft 365 Business helps safeguard corporate data against unsanctioned disclosure by helping your organization classify, label, and protect documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination where users are given recommendations.

To meet compliance standards, Microsoft 365 Business helps organizations meet compliance standards by supporting Data Loss Prevention (DLP) policies. You can create and manage a DLP policy that helps you identify, monitor, and automatically protect sensitive information across your organization.

How Microsoft 365 Business helps keep your business secure

- Helps prevent sensitive information like social security numbers and credit cards from intentionally or unintentionally leaking outside your business
- Lets you configure policies to classify, label, and protect data based on its sensitivity
- Provides persistent protection that follows your data everywhere
- Helps you share data safely with coworkers as well as customers and partners
04.

Help protect your users from external threats
New malware campaigns are being launched every day. So how do you protect your email, files, and applications against unknown and sophisticated intrusions? Microsoft 365 Business helps protect your data and devices against external attacks, including phishing, malware, ransomware, and zero-day exploits.

**Here’s how it works**

Microsoft 365 Business includes Advanced Threat Protection (ATP), an advanced cloud-based email filtering service that helps protect against unknown malware and viruses. ATP includes features to safeguard your organization from harmful attachments and links in real time, and it also has rich reporting capabilities to provide insights into the kind of attacks happening in your organization.

Microsoft 365 Business also protects your devices from viruses, malware, spyware, and other threats by enforcing Windows Defender protection for all your Windows 10 PCs. Windows Defender uses real-time protection to scan apps that your users run or sites they browse on Microsoft Edge.
How Microsoft 365 Business helps keep your business secure

- **Scans** email attachments with sophisticated techniques that detect new types of malware
- **Helps protect** against phishing and malware by automatically checking links in emails and documents in real-time
- **Helps** you apply policies that ensure Windows Defender is scanning all Windows 10 PCs in your business
- **Makes sure** devices are configured consistently to help ensure that data and devices are protected
05.

Have peace of mind that you’ve got access to your data
Just as some organizations face regulatory requirements for protecting data, many companies also need a way to archive data that solves compliance and regulatory requirements. Microsoft 365 Business helps maintain access to your data, enabling unlimited cloud archive and long-term preservation policies to ensure you don’t lose an email.

## Here’s how it works

If your company ever faces a reasonable expectation of litigation, you’re required to preserve electronically stored information (ESI), including email and documents relevant to the case. Microsoft 365 Business helps keep you in compliance without impacting productivity.

Exchange Online Archiving creates a cloud-based archive mailbox alongside your primary mailbox folders, and it can be accessed and searched just like a primary mailbox. Legal hold can help preserve content beyond emails, retaining any and all relevant content, including from Microsoft Teams, SharePoint, and OneDrive for Business. eDiscovery gives you the ability to search for the relevant content and export it for legal teams to evaluate.
How Microsoft 365 Business helps keep your business secure

› **Helps protect** archive mailboxes with advanced, dependable security measures, both physical and digital

› **Enables you to host** your archives on trusted Microsoft servers while maintaining control over your environment

› **Keeps** users productive with easy-to-use, business-class archiving
Ready to help secure your organization with Microsoft 365 Business?

You’ll find more information in the Crash Course in Microsoft 365 Business

©2018 Microsoft Corporation. All rights reserved. Microsoft Windows, Windows Vista and other product names are or may be registered trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this document. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.