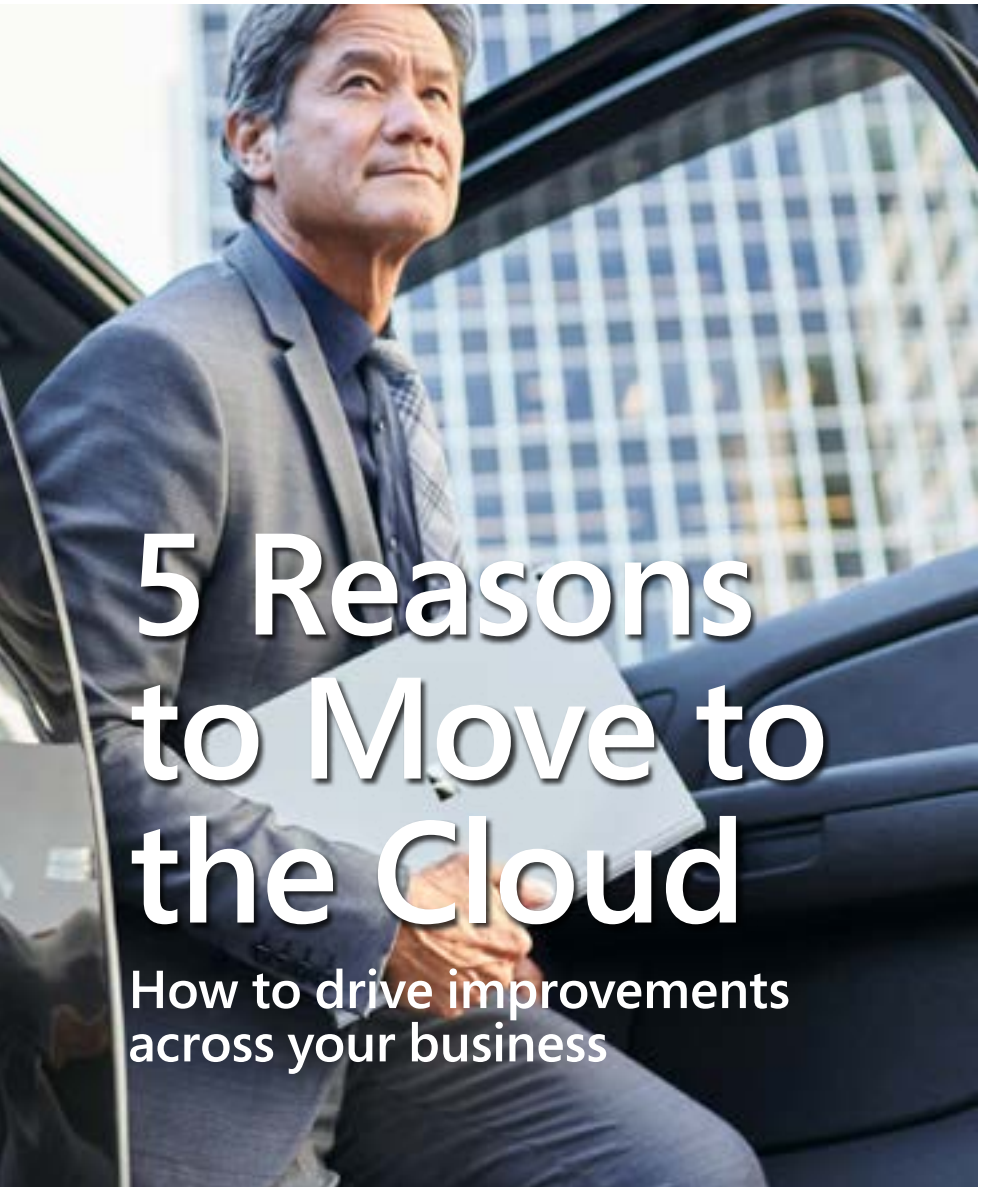
Office 365



5 Reasons to Move to the Cloud

How to drive improvements across your business

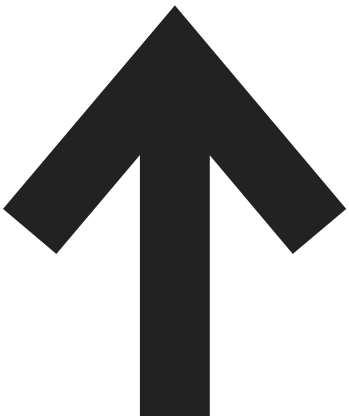
Microsoft

Introduction

Even when you're confident that a move to the cloud is good for your business, it's natural to have questions and concerns about making the change. After all, if your business is running effectively with on-site technology, you'll likely want to learn more about the security and payoffs from a cloud-based suite of tools before taking the next step.

You may want to know: Will your critical business assets be protected? Will mobile, cloud-based apps be embraced by employees? Will the tools allow them to contribute more effectively to the success of the business? Are there advantages to choosing an integrated set of technologies? Can working in the cloud improve security?

Use this eBook to get answers to these questions and explore the ways Office 365 can help your company.



01

How the Cloud Keeps Your Mobile Workforce Engaged

02

Using Office 365 to Solve Mobile Work Challenges

03

Protecting Your Digital Assets: How the Cloud Becomes a Vault

04

Guarding the Email Inbox

05

How Office 365 Helps Teams Share Data More Securely

01

How the Cloud Keeps Your Mobile Workforce Engaged

Your employees arrive at work carrying powerful computing devices connected to tools that simplify and enrich their personal lives. Do their professional lives get the same boost from the technology they use in your business every day?

Businesses are increasingly driven by employee-related benefits when they incorporate personal devices into the workplace technology mix. **A recent survey[1] of tech professionals** found that the top drivers for BYOD programs are enabling employee mobility, satisfaction and productivity.

[1] Crowd Research Partners, "**BYOD & Mobile Security, 2016 Spotlight Report**," March 2016 (Licensed under a **Creative Commons Attribution 4.0 International License**).

"The top drivers for BYOD programs are enabling employee mobility, satisfaction and productivity.

Providing your team members with cloud-based communications and productivity apps — accessible via smartphones, tablets and laptops — allows them to tackle work tasks using digital tools they are already familiar with. That eases user adoption and training issues for IT.

But there are other good reasons to consider mobile tools powered by the cloud. They can help your business in these four ways:

- **Anywhere, anytime communication to quickly respond to customers, partners and co-workers.** Communication tools that are at hand let employees alert each other to pressing challenges, move projects forward and resolve issues faster. Many already use a variety of ways to connect with friends and family — videoconferencing, screen sharing and instant messaging are as natural to them as email and voice calls. Having access to a range of business-ready modes of communication helps them do their jobs more effectively.

  Essential tools to provide: Skype for Business, with conferencing, including voice, screen sharing, video communications and instant messaging.

- **Flexibility for employees to choose the best way to get the job done.** Mobility-enabled workers can adjust workflows and tasks on their to-do lists and get them done in the right place at the right time. When employees are not tied to a specific location, it's easier for them to stay productive while balancing multiple priorities in their lives. If employees can move tasks forward when they are away from the office, they are better able to juggle personal responsibilities that arise. Life happens, but that doesn't mean work has to be derailed.

  Essential tools to provide: Productivity suite applications (Word, Excel, PowerPoint) for mobile devices.

"Fast access to timely, relevant information helps employees do their best work.

- **Opportunities for more productive teamwork.** Fast access to timely, relevant information helps employees do their best work. The ability to share and edit one copy of a single document that is stored in the cloud — rather than, for example, emailing copies of files — makes it easier to quickly share everyone's best ideas. Team members don't lose time tracking multiple versions, but instead can work together using the most up-to-date information. That results in a more responsive organization — for customers, for business partners and for your internal teams.

  Essential tools to provide: Cloud storage and file sharing (OneDrive for Business).

- **A work environment that attracts — and keeps — talented people.** Younger employees, more than any other group, may expect to use mobile technologies at work. In fact, a Pew Research Center study[2] reports that 92 percent of adults aged 18 to 34 own a smartphone. Adopting cloud-based tools helps make your business more attractive to the next generation of workers. And employees of all ages want to keep their skills sharp by working with the latest productivity software. Providing cloud-based tools that are updated with current features ensures that your workplace offers them the opportunity for continued growth.

  Essential tools to provide: Mobile email and calendar (Outlook) with system-level security safeguards that support a BYOD policy[3].

[2] Pew Research Center, "Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies," February 2016.

[3] Microsoft, "Introducing Built-in Mobile Device Management for Office 365," October 2014.

By making mobility central to your business, you are helping your employees be more productive and giving them the chance to find new ways to make your business run better. You make your business a more compelling place to work. And you give your mobile workforce the same convenience, speed and flexibility that they expect from their personal technology.

What Millennials Want: Technology that Enables Purposeful Work

In fewer than 10 years, **one in three American workers**[4] will be a member of the millennial generation. These employees — born between 1980 and the late '90s — bring a new set of experiences and expectations to the workplace.

Millennials typically want frequent feedback, opportunities to make a difference, and knowledge that their work in some way contributes to the well-being of society and the planet.

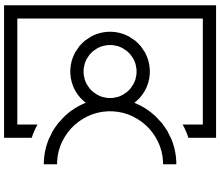
What should your company keep in mind when it comes to attracting, retaining and managing millennials? A recent **Microsoft survey**[5] of this generation found:

- **Millennials expect to use the latest tech.** Almost all the millennial workers surveyed — 93 percent — said working for a company with updated technology, services and solutions was important to them; 48 percent said it was "extremely important."
- **Mission matters.** Eighty-eight percent of respondents said evidence of a strong mission and values draws them to a company.
- **They own their careers.** Eighty percent believe they are in charge of creating their own career paths; less than half expect to stay with their current employer for more than four years.
- **Collaboration is key.** Among factors that contribute to their ideal workplace culture, people chose "good team collaboration" more often than any other.

[4] U.S. Dept. of Labor, Bureau of Labor Statistics, **"Labor Force Projections to 2024: The Labor Force Is Growing, but Slowly,"** December 2015.

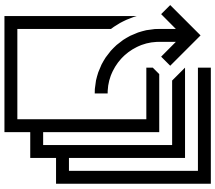
[5] Microsoft, **"The World of Work Is Changing: Millennials and Mobile Technology at the Center,"** February 2016.

02
Using Office 365 to Solve Mobile Work Challenges



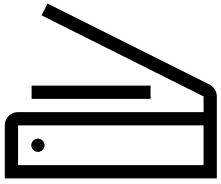
1 **The problem: A senior sales rep is preparing a presentation before leaving to visit an important client.** As she's finalizing the PowerPoint deck on her PC, she finds that she's missing a photo of the company's redesigned product as well as some revised specs.

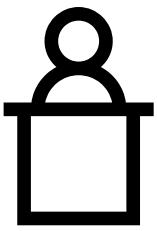
2 **She contacts a marketing manager back at the office,** using Skype for Business. He promises to locate the image and offers to add the information to her presentation while she's driving to the meeting.



3 **The sales rep shares her presentation** with the marketing manager using OneDrive, giving him rights to edit the file. She packs up her computer and gets in her car.

4 **The marketing manager scans a photo** of the new product, then opens the sales rep's PowerPoint file and inserts a new slide with information showcasing the product.





5 **The sales rep has arrived at the client meeting.** She accesses her updated slide deck from her Surface tablet and is able to give the client an informative briefing covering her company's updated product line.

Results:

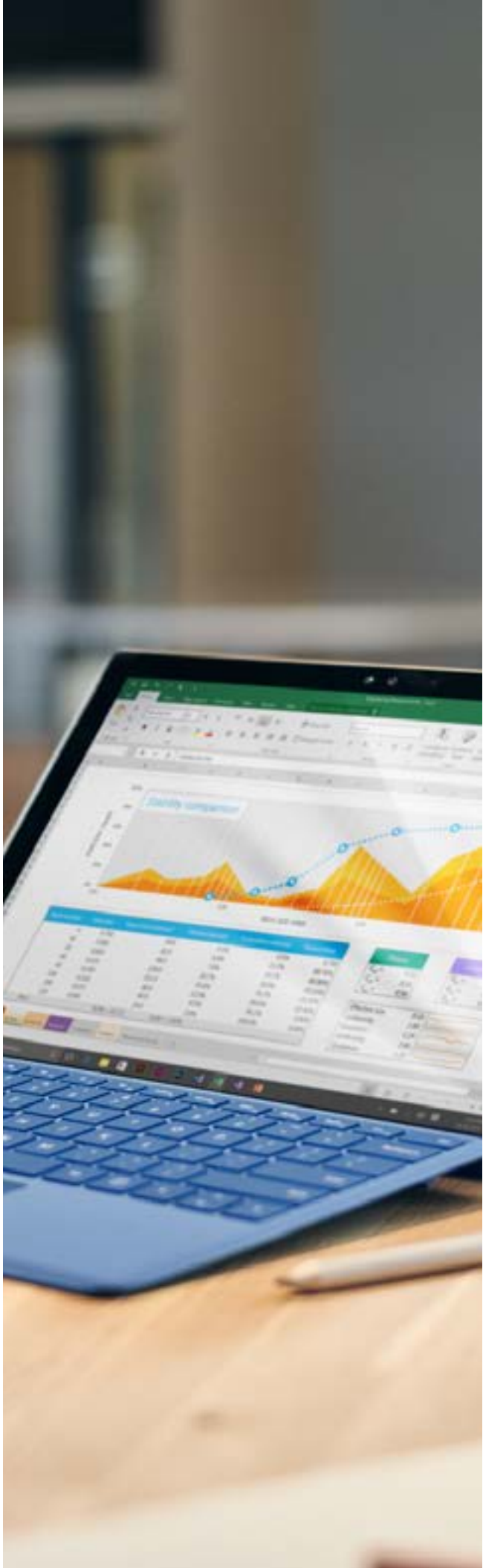
- Team members in different locations communicate and collaborate seamlessly.
- Information is easily accessed on the right device at the right time.
- The business solves an urgent problem quickly.

03

Protecting Your Digital Assets: How the Cloud Becomes a Vault

Many IT leaders are worried about security as they consider moving from on-premises computing to the cloud: More than half of the 2,200 technology executives, managers and practitioners in **a recent poll**[6] named security concerns as a barrier to cloud adoption.

The reality is that it's no longer safe to assume a company can manage every aspect of IT security in-house. In fact, with new cybercrime threats emerging constantly, companies of all sizes can find it challenging to muster the resources needed to maintain strong defenses. The best cloud services providers, on the other hand, have sophisticated safeguards in place that make them powerful allies to businesses.



6 Crowd Research Partners, **"Cloud Security, 2016 Spotlight Report,"** May 2016 (Licensed under a **Creative Commons Attribution 4.0 International License**).

"Only those with permission should have access to your applications and data.

When your digital assets are in the cloud, you need assurance that three major areas of risk will be managed: the infrastructure that the service is running on, the cyberthreat environment, and end-user accessibility to company data. Here's a close-up look at how Office 365 works with you to meet the challenge.

Cyberthreat protection

Email attachments and websites can carry a number of threats — including spam, viruses and malware — that may spread harm throughout your organization.

Office 365 offers strong protection against such threats with **Exchange Online Protection**, a service that analyzes attachments for malevolent content and helps prevent users from following malicious website links contained in emails. Managers are able to set policies that record which email recipients are following bad links so they can quickly zero in on the problem and find a solution.

Within its cloud data center infrastructure, **Microsoft** also follows an incident response process in accordance with U.S. National Institute of Standards and Technology protocols. Its security incident response organization includes several dedicated teams that work to prevent, monitor, detect and respond to security incidents. Post-incident activities include reviewing incident responses to see if protocols should change.

Controlling user access

Only those with permission should have access to your applications and data — and in a cloud-based system, just like an on-premises implementation, you need to be able to set your own controls. If your company permits or encourages BYOD, that adds another dimension to managing and controlling access.

Office 365 uses Azure Active Directory to manage users and provide authentication, identity management and access control. The capabilities include a cloud-based store for directory data and identity authentication services such as user logon processes. These services are designed to integrate with your on-premises Active Directory implementations and fully support third-party identity services. Your Office 365 administrator can enact multi-factor authentication to provide extra security through a mobile app, phone call or text message. And **Microsoft Intune** mobile device management enables you to protect sensitive data and prevent its loss on devices across Windows, Apple iOS and Android platforms.

Securing your digital assets in the cloud is ultimately a partnership between you and your cloud provider. With Office 365, Microsoft has built a robust defense of the data center, while giving IT professionals the tools to control user access and manage mobile devices. For more details, visit the **Microsoft Trust Center** and download our **Office 365 Security and Compliance** white paper.

Nine Security Questions to Ask Every Cloud Services Provider

When you're evaluating a cloud offering, you want to know it offers the security and service level you need to keep your business running. Ask these nine questions — and be sure you are satisfied with the answers — before you pick your cloud services provider.

1. Where do you keep our data?

The cloud is a distributed IT environment, so providers can mitigate risk by keeping copies of data in more than one place. That means a major problem at one location won't spell failure for all locations. Make sure your provider's data centers are geographically dispersed.

2. What actions have you taken to physically secure your data centers?

A cloud provider should be able to explain how the construction of its data centers meets standards for protection against natural disasters, including a description of high-availability and failover capabilities. It should also be able to discuss physical security features, such as perimeter fencing, security guards and video surveillance.

3. How do you keep our data separated from that of other customers?

Cloud providers design their systems to serve many customers simultaneously. Ask your cloud provider how it maintains the integrity of your data — documents, email messages and application data — in a multi-tenant computing environment.

4. When do you encrypt our data?

Confirm that your data will be indecipherable to unauthorized parties at all times — when it is stored, when it is being processed in an application and when it is sent over a network.

5. Who at your company has access to our data?

Cloud providers may automate many of their IT systems management operations in order to limit internal security risks, but some tasks may require human access. The provider should describe which job roles have permission and how access is tracked, monitored and audited.

6. How do you handle network and information security risks and any incidents that may occur?

Cloud providers following best practices can describe their process for detecting and responding to threats, including how they contain malware incidents and remedy any security breaches. As a follow-up question, ask what industry or government security standards the cloud provider follows.

7. What kinds of controls and monitoring tools will we have?

Your cloud provider should provide administrative controls that allow you to manage your users' access to email, applications and data across multiple types of devices. You should also be able to monitor system performance in the cloud. Follow-up question: How does it enable multi-factor authentication and third-party identity management providers?

8. How do you ensure that software applications are secure?

Your cloud provider should detail its quality assurance capabilities for the applications it hosts, including software development and ongoing procedures to address vulnerabilities as they arise.

9. What is your uptime guarantee?

Cloud providers typically offer a service level agreement; for example, Microsoft offers commercial customers a **99.9% financially backed uptime guarantee**. Ask if the provider publishes any historical reports on service uptime (**Office 365 uptime reports** are released quarterly).

04
Guarding the Email Inbox

A well-meaning employee receives an email with an attachment that looks important, so he or she opens it. Suddenly, your IT team is battling a malware outbreak.

Forty-three percent of small and midsize businesses have encountered a phishing or social engineering attack, according to a 2016 **Ponemon Institute survey**.[7] Cybercriminals have gotten very good at fooling people: An experiment conducted by **Carnegie Mellon University**[8] found that on average, users were able to correctly identify just over half of malevolent emails received. That means it's essential to have updated tools to mitigate your risk.

Office 365 offers **Exchange Online Advanced Threat Protection** (ATP), an email filtering service that provides system administrators with information about attacks as they occur. The service includes:

- **Sequestering malevolent content.** Microsoft Safe Attachments performs a real-time behavioral malware analysis to screen out malicious content before it reaches recipients.
- **Filtering website links.** Exchange Online Protection scans content to identify malicious website links. Microsoft Safe Links expands on this service by examining URLs as a user clicks on them. If a link is rated as unsafe, the user is warned or informed the site is blocked.
- **Monitoring system risk.** ATP's reports help IT administrators track which users clicked a malicious link and when. It highlights who is targeted, and by what types of attacks. It also enables IT to investigate suspicious messages and malicious links.

[7] Ponemon Institute, "**2016 State of Cybersecurity in Small & Medium-Sized Businesses,**" June 2016.

[8] Canfield et al, **"Quantifying Phishing Susceptibility for Detection and Behavior Decisions,"** Human Factors: The Journal of the Human Factors and Ergonomics Society, December 2016.

05

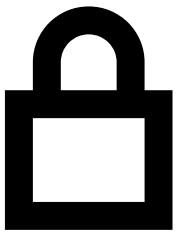
How Office 365 Helps Teams Share Data More Securely

1 **The company's controller is working late from home**, finalizing the past quarter's financial statements in time for the CEO's meeting with investors tomorrow. But in reviewing Excel spreadsheets, he's found a discrepancy between revenue booked and reports of sales closed.

2 **He sets up an emergency conference call** over Skype for Business with the sales operations manager and the bookkeeper to discuss the conflicting information.

3 **The bookkeeper accesses accounting records** via OneDrive, using two-factor authentication for more secure access to sensitive company information, while the sales manager accesses his records.

4 **The team discovers** that revenue from a new account was incorrectly booked into the current quarter instead of last quarter. The bookkeeper fixes the error.



5 **The controller accesses the corrected spreadsheet** and updates the income statement. He encrypts the file, protects it with a password that will provide read-only access to the file, and emails it to the CEO. The early morning investor meeting can go forward without a hitch.

Results:

- Colleagues can quickly solve a problem through an emergency virtual meeting.
- Authorized users can securely access sensitive information, even away from the office.
- Critical business data can be protected from editing and safely transmitted.

Office 365

How we work has changed. How do you know that you're making the best use of technology to make your business as efficient as possible? Register Now for a 30-minute visual demonstration of Office 365, and learn how it can propel your business to new levels of productivity.

Microsoft