



# Microsoft 365: The Secure Way to a Digital Future

**Like many trends**, the move to a digital workplace began with a trickle as companies sought to implement a better disaster recovery system, cut spending on hardware, or find a more flexible way to scale. Then came the BYOD revolution. A host of apps found their way into businesses, each with its own operating system for an overburdened IT department to manage (or discreetly ignore), and its own often subpar security. At the same time, ecommerce companies began gathering troves of data to give customers the fast, personalized experience they have come to expect everywhere.

Digital transformation is now reaching critical mass, and any company that wants to remain competitive must provide both workers and customers with a flexible, cloud-based, efficient, and highly secure way of doing business. By the end of 2019, digital technology spending is expected to reach \$1.7 trillion worldwide, a 42% increase from 2017, a recent [IDC study](#) found. By 2020, 60% of enterprises will be implementing a full-scale digital strategy. They will have to, because by the same year, [92% of all workloads](#) will be processed in the cloud.

Yet many companies are approaching digitization piecemeal, with a file-sharing app here and a storage provider there instead of an integrated strategy. That approach won't cut it in today's environment, where competitors have sophisticated cloud-based business models. As a [Gartner analyst](#) put it, "digital projects are not a digital business." The IDC study found that 59% of companies remain at "stage two or three" of digital transformation maturity, a phase the company calls "digital impasse." Two-thirds of business leaders know their companies need to pick up the pace of digitalization to remain competitive, Gartner said—but too many just aren't getting it done.

What's holding them back? It can be tough to make spending decisions amid a vast array of options, and many companies worry about security. But dipping a toe here and there results

in a mishmash of disjointed technologies that may not work well with one another, let alone with the enterprise systems you already have. It creates a management nightmare for IT and a jarring experience for employees, who waste time devising workarounds for systems that just won't sync.

To meet the digital future, businesses need a single, comprehensive technology with a fast, reliable operating system; seamless enterprise-wide collaboration and mobility; and state-of-the-art security. That technology exists today in a platform with many elements you're already familiar with. It's called Microsoft 365.

## An Integrated, Secure Platform

Microsoft CEO Satya Nadella calls Microsoft 365 "the coming together of the best of Office 365, Windows 10, and enterprise mobility and security." Available for both small and midsize businesses and enterprises, Microsoft 365 is a complete, integrated solution that helps workers become more productive, collaborative, and creative while providing the best possible security for your data at all times, whether workers are at the office or on the go. Here's a rundown of some of its most important features.

## Office 365: Built for Mobility

Office 365 takes Microsoft's powerful productivity suite to the next level. In addition to offering updated versions of Word, Excel, PowerPoint, Outlook, OneNote, Publisher, and Access—programs that millions of workers have relied on for years—it includes Microsoft Exchange Server to coordinate email and calendars, and SharePoint, the web-based collaboration platform that integrates with all Office products.

But the emphasis on collaboration and mobility doesn't end there. Office 365 also includes OneDrive, which allows workers to securely share Office files from anywhere via a mobile app.

With OneDrive, used by 85% of Fortune 500 companies, you don't have to worry about transferring big PowerPoint files or bulky Excel spreadsheets by email. Workers get instant access to them through the app, and anyone with permission can make changes. Files are automatically synced so that everyone always has the latest version.

Office 365 also includes Microsoft Teams, a collaboration platform that allows groups of employees scattered across a city—or across the globe—to have chat sessions, voice conversations, or videoconferencing through Skype, during which they can also share and collaborate on documents. Employee groups can create their own channels within Teams for specific projects or topics, with easy access to relevant chat threads, documents, apps, and files.

Office 365 runs on Windows, Mac, Android, iOS, and web platforms, so anyone can access it anywhere. That's crucial in a world where [43% of people](#) work remotely at least sometimes and employees spend as much [as 80% of their time](#) collaborating with others. Office 365 confronts the reality of sharing and mobility head-on, giving workers dozens of ways to come together and use rich tools to complete projects faster.

## Windows 10: Easy Management, Creative New Features

Mobile-friendly Windows 10 integrates smoothly with smartphones and tablets, allowing users to interact with their devices in new ways, including voice control, digital pens, touch, and gesture commands. It also includes the digital assistant Cortana, which can help employees manage their schedules, locate files, and dictate emails to save time.

Windows 10 reintroduces the Start menu for easy orientation and lets users set up virtual desktops. You can also run multiple operating systems on one Windows device as virtual machines with Client Hyper-V.

Configuring settings for mobile access and security is fast and simple. Updates are automatic—unless you'd prefer to defer them and set your own schedule. With easy controls for IT and an intuitive, fun experience for users, Windows 10 now runs on [600 million devices](#) worldwide.

## Enterprise-Grade Security

For businesses, one of the strongest features of Microsoft 365 is its state-of-the-art security. Windows Defender uses AI techniques to provide advanced threat protection, discovering and removing malware before it can infect your network. It allows IT to see configurations and patch status for endpoints across the enterprise. A [Forrester study](#) found that Windows Defender catches 1.7 times as many threats as competing tools, and reduces the risk of a data breach by 40%. It discovers threats and eliminates them four times faster than other tools.



Windows Hello gives you multifactor and biometric identification to keep unauthorized users out. In addition, you get encryption through BitLocker—and BitLocker To Go for USB drives—to keep your data safe if a device is lost or stolen. You also have the ability to remotely wipe company data from any device while leaving the user's own apps and information intact.

You can protect company information at the app level by setting access policies based on user identity and their need to view sensitive documents. Conditional access ensures that no users, apps, or devices can access Office 365 data unless they meet your company's compliance requirements.

No matter how much employees clamor for mobility, it is worthwhile for businesses only if it can be implemented securely. With Microsoft 365, intelligent threat analysis combined with customized sign-on and access policies provide protection that lets you sleep at night while giving employees the freedom to share and collaborate anywhere, 24/7.

## Planning for the Future

Digital transformation is not a once-and-done affair. It continues to evolve as new technologies develop, including the Internet of Things (IoT). As systems like Windows 10 become popular, support for older versions is phased out. If you don't keep up, you can expose your organization to serious security threats, such as the [WannaCry ransomware attack](#) that hit over 200,000 computers running on old versions of Windows.

Cutting-edge security is an important reason to move to Microsoft 365 sooner rather than later, but it's not the only one. Office 365's rich arsenal of tools and mobile-friendly features allow your workers to compete in an environment of increasing demands for productivity gains. Windows 10 offers you unprecedented ability to manage distributed teams and configure appropriate settings for all classes of workers or contractors. A secure, comprehensive, integrated solution, Microsoft 365 has you covered as you move your company to a brighter digital future.

---

**Learn how Connection can help you empower your digital workforce with [Microsoft 365](#).**

## ADDITIONAL READING

# Why 2018 will be a year of acceleration for workplace transformation

The digital workplace transformation is clearly underway and in 2018 we expect to see IT help enterprises shift these ideas from concept to reality

By Stephanie Hallford  
Contributor, CIO | DEC. 2017



The rise of digital business has ushered in a broad array of advanced technologies to help people work more efficiently. But not all organizations are keeping pace with the rapid transformation of the workplace from a physical to a digital space.

So, who is at the leading edge of the transition? So-called “smart” offices — these are the organizations where the majority of talented people want to work. In fact, more than half of today’s workers are [concerned that their office environments are not advanced enough](#). If you work in such a place, while your associates at other companies constantly tell you about the cool technologies at their fingertips, you know the feeling: frustration.

Fortunately, many companies are catching up rather than losing out. Businesses everywhere are exploring the full complement of digital work technologies that help workers achieve higher productivity, greater collaboration, and more data moves through organizations — hallmarks of the transformation. Setting the stage for these advancements are relentless efforts to boost performance at the edge of the enterprise. Just as organizations seek to empower their workers with the tools to process larger analytics workloads, IT also recognizes the urgency of providing continuous security — no matter where the work is performed.

We see 2018 as a watershed year, in which new technologies will transform many more companies into smart and data-driven workplaces. And we believe three key trends will shape the new digital work environment.

## 1. IT will implement endpoint security solutions such as multifactor authentication to protect the mobile enterprise

As IT departments build out these virtualized smart offices, they will also focus on enhancing endpoint security solutions that protect the digitized, mobilized enterprise from cyberattacks and intrusions. We are now in a global climate of “in” security, with a threat landscape that’s growing exponentially. The freedom to work from any location outside of one’s office network requires a new approach, with more focus on secure remote solutions to ensure that what employees send, receive and launch from their devices will keep them safe and not jeopardize their clients, partners, co-workers, or their organization’s IP.

Stronger endpoint security is complex and evolving, however one important means is via the use of authentication protocols that go beyond software. Multifactor authentication (MFA) that is built into hardware is one proven way to combat cyber breaches. Optimizing endpoint security requires embedding authentication into silicon, which provides a layer of hardwired protection much tougher to hack than software alone. While everyone is on edge about the risk of cyber threats, new generations of biometric sensors that very accurately identify – and ultimately protect – trusted users are just beginning to gain widespread acceptance. And without trust, there can be no smart office.

## 2. Workplace transformation will accelerate

Organizations will embrace a full complement of new technologies to retrofit their offices, including technology that enables [faster processing of data workloads](#). Data-driven productivity that taps into strong edge computing along with the cloud is an exciting development that may help foster a workplace culture of deeper data analysis highlighted by richer business insights that once required dedicated IT resources. Empowering the workforce with data-driven knowledge increases their ability to make more strategic contributions.

[Read more](#)



## ADDITIONAL READING

# Why 2017 is the year that changed Windows management forever

**In fact, it may have been the single most significant year yet.**

By Sumir Karayi

Contributor, Computerworld | NOV 2017



2017 was a truly transformative year in the history of corporate IT. I would even go so far as to say that, in my 25-year history working with Windows in large organizations, I think this has been the single most significant year yet.

The transformation has been the realization that the way we think about every aspect of Windows management, from minor change to full-scale migrations, has to change. It's worth repeating that the instruments of this collective revelation were WannaCry and NotPetya, which caused some of the worst damage I have seen in my career, so much so that I now think disaster planning must take such attacks into account.

For most CIOs, CTOs and even CFOs, the penny likely dropped in the time it took to discover that a significant proportion of the UK's National Health Service's IT infrastructure had been compromised – because of an outdated operating system and the fact that NHS ignored simple security best practices.

I speak with 5-10 companies a week about their Windows strategies, and they all agree with the following statement: there is no point in worrying about expensive alarm systems (in the form of security products), while leaving the front door and windows wide open by not keeping software current.

Staying current has become fashionable, and it's one trend I can totally subscribe to.

## Meanwhile, in Redmond

For those organizations that had already taken the hint and made the large commitment of transitioning to Windows 10, they found themselves in a world that was very distinct from the one they had left behind.

With Windows 10, every six months effectively requires (and compels) a full OS update. Currently, most organizations are used to doing a full Windows upgrade every six or seven years, sometimes even longer. While CIOs might not like the new rapid pace of updates, this is a change for the better.

For far too long, Windows has been an insecure operating system (sometimes ridiculously so), with hackers able to rely on the very simple mechanism of monitoring common vulnerabilities. All they have to do is look at security research, which points out vulnerabilities. Some even provide code examples, so the hacker just needs to repackage the code into a delivery mechanism.

Unless you're tending to the underlying operating system as well, patches are just a bandage. In Windows 10, Microsoft added 17 major security enhancements and the list of common vulnerabilities is significantly lower. The faster update cycle for Windows 10 — assuming organizations keep up with those updates — will help ensure that they are never as vulnerable as they were in the past.

## What this means

The way we used to work — with one massive migration project every few years — is out the window (as it were). Organizations are likely to stay current once they move to Windows 10.

The fly in the ointment is that Microsoft hasn't given sufficient attention to how third-party applications fit in with this vision. Given that we use Windows to run applications, it is essential we take them into consideration.

[Read more](#)

---

**For more information about the comprehensive services  
Connection offers, contact your Account Manager today.**

Business Solutions  
**1.800.800.0014**

Enterprise Solutions  
**1.800.369.1047**

Public Sector Solutions  
**1.800.800.0019**

**[www.connection.com/Microsoft](http://www.connection.com/Microsoft)**

©2018 PC Connection, Inc. All rights reserved. Connection® and we solve IT™ are trademarks of PC Connection, Inc.  
All other copyrights and trademarks remain the property of their respective owners. C695352 0118

