Building a hybrid workplace with less

How Noventiq, Microsoft 365, and Microsoft Intune can help you enable hybrid work with less cost, deployment time, and risk

Introduction

The workplace is changing fast. Maintaining a competitive workplace means meeting new needs, particularly when it comes to hybrid work. The pandemic may have brought the hybrid workstyle into the limelight, but since then this model has more than proven itself—this is how people want to work today, and that's actually good news for you.

A recent study by **Forrester** from October 2022 shows hybrid work improves user productivity by an average of 60 hours per year, while saving businesses 25 percent on travel costs and decreasing most organizations' physical footprint[1]. But perhaps the most compelling advantage is being able to attract quality workers in a time when recruiting and hiring is more challenging than ever. More than 58 percent[1] of job candidates say they want a hybrid or entirely remote working arrangement. So, the question isn't whether or not to build your hybrid workplace, it's how you can build it efficiently, effectively, and securely.

Meeting those criteria means you'll need to focus on three key components: (1) A simplified management tool set so IT can respond fast and do its job effectively; (2) Strong, agile security measures to protect data and workers over the cloud's much larger attack surface; and (3) Building the best user experience possible so employees can realize all the productivity benefits that hybrid work brings to the table.

Noventiq and Microsoft 365 can not only help you meet all these needs, you'll do so while building a powerful, advanced hybrid work solution that supports today's workforce demands. Even better, you'll do it with less cost, deployment time, and risk, of having **Noventiq** by your side.

Today's workplace challenges:

Cyber-attacks are more sophisticated and constantly evolving

New devices and workstyles drop new burdens on IT's shoulders

An uncertain economy dictates a need for continuous agility and cost savings

# Easier IT management from anywhere, on anything

Next to security, one of the most challenging aspects of hybrid work is that it's device agnostic by nature. Businesses can't control the devices employees will use when they're working remotely. That means IT is faced with supporting more devices than ever—from phones to tablets and back to the traditional PC. Even more challenging, they'll often be supporting those devices across long distances instead of standing at the employee's desk.

Left to fend against this problem on their own, IT workers will default to whatever help they can get their hands on, which means a much bigger and more confusing tool set that not only takes long to learn but is also more difficult to use and not always reliable.

Microsoft Intune, which is included in Microsoft 365 Enterprise, makes those problems a non-issue. The same stack that gives your employees one of the most recognized productivity platforms in the world also gives your IT professionals a set of management tools designed

specifically for cross-cloud scenarios. It's easy to learn and using it will let your IT department protect users, data, and the broadest array of devices possible, including Windows, Android, Apple's iOS and macOS, and even Linux.

Intune gives your IT staff all the tools they need to provide users with an effective, consistent remote support experience. They'll be able to onboard different kinds of devices themselves using the same familiar procedures, while IT can easily deploy pre-configured operating systems and applications. IT will be able to auto-enroll new users and equipment into the right user and team groups, collaborative discussions, and data repositories from the very first login.
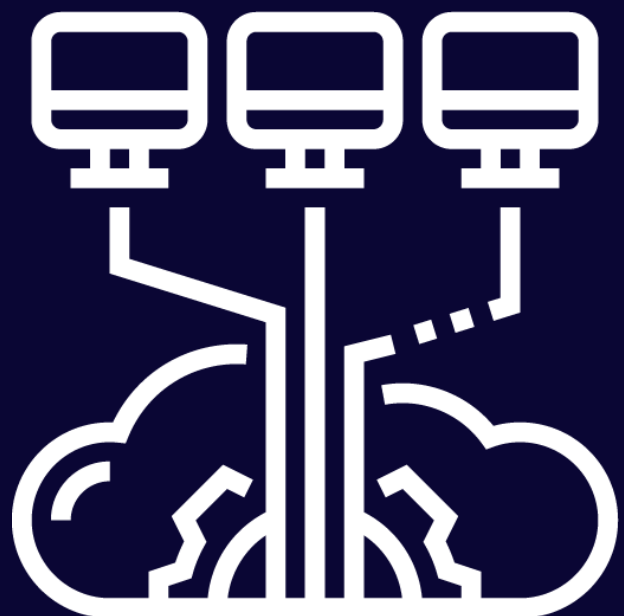
Intune also enrolls users' devices into Windows Autopatch, which does away with update-related distractions so your IT staff can focus on more valuable work. It reduces endpoint vulnerability for any Windows device by ensuring the right security updates are installed automatically, while providing IT with constant visibility to monitor, test, or rollback updates as needed.

Microsoft 365 also lets you deliver new Windows experiences to your users while still leveraging the same management tools and IT skills you already have. As an add-on to Microsoft 365, Windows 365 runs entirely in the Microsoft Cloud, so users can access virtual Windows 11 work

environments on any device with a browser and an internet connection. The service includes timely patching and updates, and your IT team can manage and customize down to the individual user level just as they would any other Windows machine.

All these components mean Microsoft 365 and Intune will give your employees and IT managers a reliable and easy to manage hybrid work experience. Workers will have complete freedom in the devices they want to use and the locations from which they want to work, all while letting you cut costs across hardware, licensing, and maintenance.

Keeping workers and data safe in a hybrid work world

Even when managing only an on-premises office environment, IT security professionals face formidable challenges today because they're battling a constantly evolving threat that's coming at them from new directions. Winning that fight in a hybrid model means they'll have to protect a much larger attack surface that also requires new expertise since it presents new gaps and vulnerabilities. And as if the complex mix of on-premises and cloud apps, varying devices, and new management tools isn't difficult enough, hybrid work often throws in new regulatory and compliance concerns.

To meet these evolving needs, hybrid-capable security pros need a robust set of management tools that protect users while maintaining a stable IT environment free from rogue devices and shadow IT. They need to find, stop, and remediate user attacks with that

Zero Trust built-in

Windows, Microsoft Intune, and Azure Active Directory can reduce the data breach risk by **45%** and overall identity management and access management costs by **50%**[2]

same tool kit, and also need to manage risk and respond to compliance and regulatory requests. That's what Microsoft 365 and Intune deliver.

With Intune, IT professionals know the health, security status, and compliance requirements of every device, operating system, or virtual machine in their purview. By combining Intune with Microsoft's Azure Active Directory, they'll be able to deliver a cutting-edge identity management platform that's easily built and monitored through the same Intune dashboard they use to manage the rest of the network.

They'll be able to implement secure access to cloud resources or on-premises apps and devices while also managing updates and patching. Because they'll be doing this proactively, your organization will also be able to avoid incidents instead of spending additional money on fixing them after the fact.

Azure Active Directory lets IT implement advanced management needs via policy to organize your organization into groups that allow for controlled access to resources. Policies let IT mandate security and compliance settings across the organization rather than user- or team-specific rules and settings. It's also a much easier way to implement single sign-on (SSO) functionality so employees won't have to juggle more than one password.

Microsoft 365 with Intune also integrates an end-to-end Zero Trust security model. Zero Trust is the most effective way to protect any network against the ocean of threats, hacks, and vulnerabilities that all companies face these days. But organizations with disparate cloud and app platforms have a difficult and constantly evolving challenge when it comes to deploying an effective Zero Trust implementation. While it works at your environment's bedrock layer touching all apps and users, if those apps constantly change or can't easily communicate with one

another, maintaining Zero Trust becomes difficult or simply impossible.

Microsoft 365 with Intune is already pre-configured, which means user identities are consistently verified using the strongest authentication methods available. It also means only verified apps and devices will have access to either cloud or on-premises resources.

Security professionals rely on the Zero Trust model because it combines the latest security methods with automation, meaning immediate alerts that let your IT staff respond and remediate much faster. A Zero Trust system also stops malicious activity from untrusted sources automatically, which means your data and workers are kept safe even if in-person IT intervention isn't immediately available. It can also revoke or lock up access to any user or resource it deems compromised or under threat. Bottom line: Zero Trust means that detection and response become proactive, and that's exactly what you need in a widely distributed hybrid work scenario.

Creating a collaborative and consistent work experience

From a frontline business manager's perspective, hybrid work has different risks than those facing IT. Executives and team managers often worry about the loss of visibility they'll face when it comes to how and when their employees are working and how effective they'll be. A winning hybrid work strategy means not just giving managers and employees the same experience they'd have in the office, but a better one.

Using Microsoft 365 with Intune, you'll build that experience with access to a single, integrated cloud-first platform that addresses all the ways people want to work today. Take transitional workers, for example. If a sales manager needs to provision devices for both permanent and temporary holiday sales staff, IT can automate the process using Windows Autopilot and Intune. These tools let IT professionals design different policies for the permanent and temp workers so

their devices will be automatically configured according to their roles. This includes the apps that get installed, the security and access privileges they get, even the device types IT wants to support. From the user standpoint, Intune will deliver a one-touch online enrollment process that'll happen automatically without interference from IT or additional input from users. Best of all, you can scale the number of managed devices up or down to get your best business outcome.

Delivering a quality user experience:

App and device health scores with endpoint analytics

Remote Help for live troubleshooting

Unobtrusive app protection with unified mobile application management

What's blocking users from such an experience today is that most organizations' current IT and software environments are fragmented and therefore difficult to learn and unreliable. That fragmentation also results in access challenges because IT can't customize devices and user roles ahead of time. Intune helps heal all those problems.

Whether it's a corporate-owned Windows PC, a user-owned portable device, or a Windows 365 Cloud PC, you'll get the same consistent management and work experience across devices. Let's say Fred is your overworked IT manager. He can breathe easier and focus on more value-add tasks since he'll be able to use Intune's Productivity Score to keep track of each employee's current work experience and resolve endpoint issues more quickly. He'll also be able to use Intune's Endpoint Analytics to find issues proactively, stopping problems before they affect users to keep employees productive.

Intune will deliver all apps securely and pre-configured for what your employees need to do. It protects access and implements a zero-touch deployment process using a frictionless, user-driven experience that also delivers constant insights and recommendations to the IT

professionals monitoring your environment. That level of transparency is critical to your ability to provide workers with a safe and consistent work experience.

Finally, Microsoft 365 is designed not just to transform how users work, but to streamline how you do business. Users will be part of a collaborative work environment that makes communication a constantly available tool. Employees will be able to find and foster new connections and conversations in ways that simply weren't available before. Using features like artificial intelligence, customizable workflows, user-designed dynamic dashboards, and much more, your workers will have the sophisticated software they need to be at their most productive, no matter where they are.

Microsoft 365 with Intune delivers a productivity stack that is both cutting-edge and proven. Its tools enhance what your employees can do while also reducing downtime from crashes or security problems—all of which lead to better business outcomes and happier employees.

Successful hybrid work with less

We've seen how a hybrid work platform built with Microsoft 365 is efficient, safe, and productive. But it's also cheaper. It lets you do so much more with so much less. Forrester finds the reason that 81 percent[1] of organizations purchase Microsoft 365 is specifically to reduce costs associated with software and infrastructure.

Take the simplified IT management experience. Not only does it let harried IT professionals catch their breath, it also helps them become more effective. They can use automation to make things like software deployment, application configuration, and device or user onboarding easy and consistent. That means less intervention and reduced help desk costs. Forrester finds that software deployment time dropped an average of 25 percent when done inside a Microsoft 365 environment. The research also showed that it decreases endpoint protection times by up to an eye-opening 75 percent and eliminates an average of 15 percent of help desk requests at the same time.[1]

Most companies suffer from too many tools for too few tasks, resulting in app redundancy and a much higher software cost than is necessary. Microsoft 365 helps consolidate a previously complex licensing structure, cutting down on consulting costs as well as deployment and integration dollars. The new features that Microsoft 365 offers both managers and workers make it easier to build a consistent experience across on-premises and hybrid work. Plus, the experience can be deployed and customized quickly with minimal training costs since workers and managers are already familiar with most of these tools.

Eliminate redundancy

Consolidate complex licensing
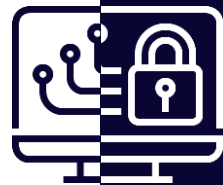
Do away with redundant capabilities using seamless, native integration

Cut consulting and deployment costs

Microsoft 365 also turns the bring-your-own-device (BYOD) problem into a cost benefit. Because it uses industry-leading multifactor authentication (MFA) technology via Azure Active Directory, users can work on any device they like with confidence and security. According to Forrester, that translates into a 23 percent reduction in what your organization needs to spend on employee devices and security.[1]

In fact, Microsoft 365 with Intune reduces the total cost of risk across your whole organization. Because the stack stops many attacks and vulnerabilities automatically, it lets your IT security professionals respond much more quickly to threats that really need their attention. And because it provides such a high degree of reporting transparency, you'll be able to respond faster to any regulatory or compliance needs, too.

All in, Microsoft 365 represents a leading solution for safe, productive hybrid work, delivering simplified management tools that help IT do its job effectively while maximizing your technology investments and decreasing costs. It protects your digital workers with the same efficacy whether they're engaged on-premises or remotely. And it gives those workers one of the most sophisticated productivity and collaboration suites—a suite with which they're already familiar and can now access anywhere, and on any device.

Turn BYOD into a cost benefit

Microsoft 365 with multifactor authentication via Azure Active Directory can reduce employee device and security costs by 23 percent.[1]

Go hybrid with Noventiq

Noventiq helps you get started on the path to a secure and productive hybrid workplace with effective endpoint management.

Noventiq is a leading global solutions and services provider in digital transformation and cybersecurity -enables, facilitates and accelerates digital transformation for its customers' businesses, connecting 75,000+ organizations from all sectors.

Join us for an Endpoint Management with Security Workshop

Noventiq's three-phase Endpoint Management with Security Workshop will help you discover the value of Microsoft 365 and Microsoft Intune for your hybrid workforce, while you learn how to simplify management and security for users' devices, apps, and identities from anywhere.

Contact us today to learn more and schedule your workshop!

1 Forrester Consulting, The Total Economic Impact™ of Microsoft 365 E3, commissioned by Microsoft, October 2022
2 Forrester Consulting, The Total Economic Impact of Securing Apps with Microsoft Azure Active Directory, commissioned by Microsoft, August 2020

NOVENTIQ
Global expertise, local outcomes