Microsoft Surface

Increase efficiency and simplify deployment with modern endpoint management

Microsoft Surface device-management solutions can help you do more with less risk, less complexity, and fewer resources.

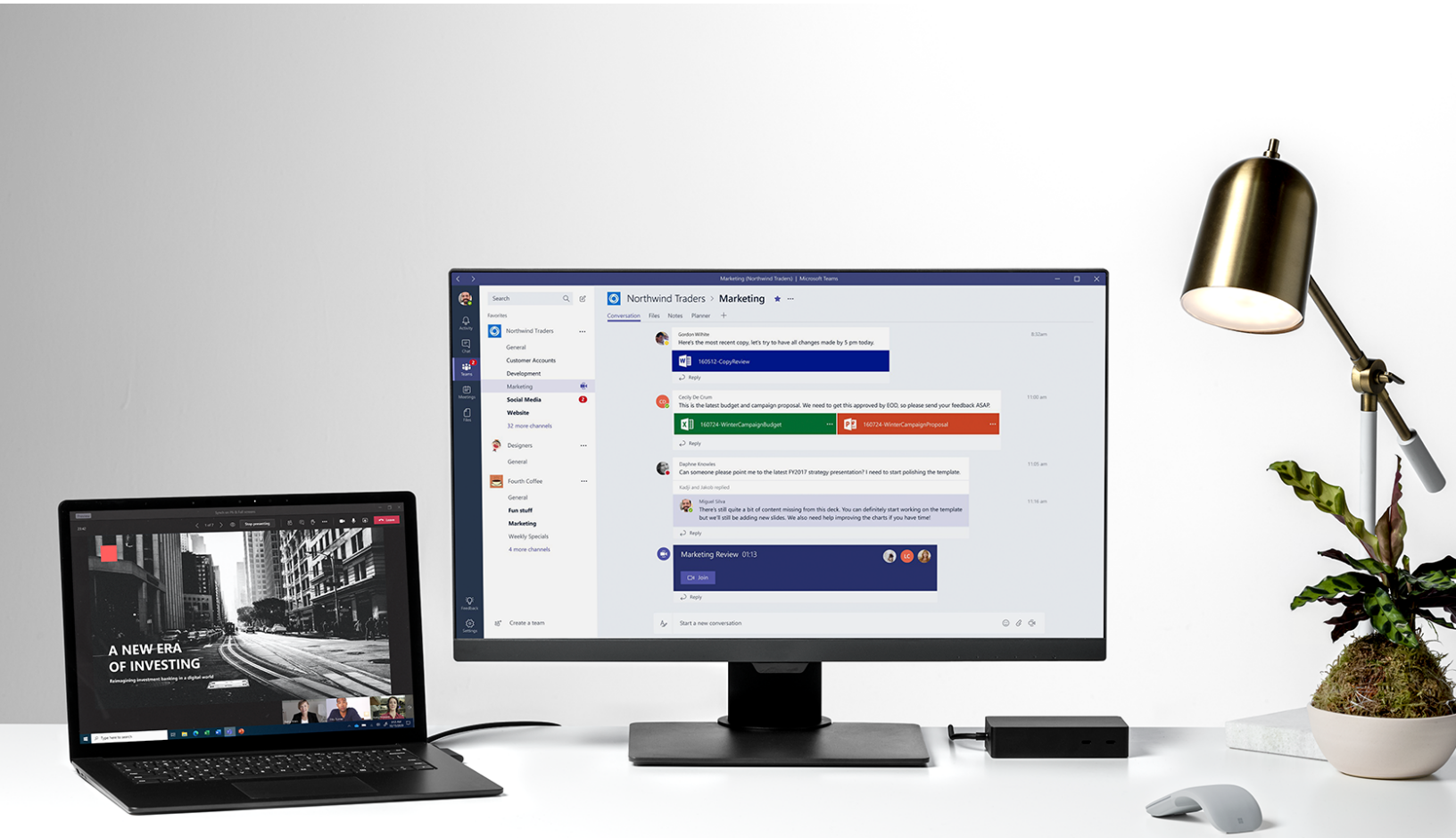

Table of contents

Estimated reading time:

15 minutes

Who this is for:

This e-book is for you if you are responsible for deploying and managing the devices that are used in your organization.

Deliver seamless, easy access to information, improve IT efficiency, and reduce risks

Today's workplace is a reflection of recent significant societal changes, where hybrid and remote workforces are becoming the norm.

Employees need to be able to work wherever they are, whenever they need. That has added new challenges for IT leaders when it comes to managing endpoint devices. Holding costs in line while helping to ensure security in this complex environment brings its own obstacles. These obstacles are exacerbated by IT often depending on a patchwork of security solutions that can be expensive and deliver insufficient levels of security. Then, there are the security challenges that come with keeping devices current and apps up to date with the latest updates and protections.

Those are among the key reasons that security is still the most urgent concern for IT leaders, with IDG's "2020 Security Priorities Study" finding that more than one-third (37 percent) of security/IT decision makers (ITDMs) say that unexpected business risks, such as the pandemic and workforce changes, are keeping them from spending time on strategic security tasks.[1] With employees accustomed to seamless access to information, whether they're using a work device or a personal device, IT teams face another layer of complexity in ensuring that every person can be as productive and secure as possible.

What's needed is unified endpoint management (UEM), a modern approach to client and device management that increases efficiency, simplifies deployment, and reduces risks. The right solution includes built-in, proactive security protections that span firmware, the operating environment itself, and the cloud.

01.

The modern model for unified endpoint management

Unified endpoint management demands a complete, streamlined view across endpoints. It also helps IT teams effectively and efficiently manage, streamline, deploy, and secure the wide variety of devices that are connecting to enterprise IT environments. The cloud has had a big impact on endpoint management's evolution, serving a pivotal role by delivering anywhere, anytime availability and advanced security. By proactively moving endpoint management into the cloud, IT teams can better maintain secure control over every connected device, prevent employee-introduced vulnerabilities, and manage devices with just a few clicks.

Traditional endpoint-management approaches have assumed that every device that IT manages is owned by the organization and connected to an on-premises network, with group policies designating user access privileges. But ever-growing threats, combined with the increased use of personal devices and the fast pace of change in IT systems and applications, have made securing all of those devices a huge challenge for IT teams. Often, too much IT time is spent reacting to threats and solving problems instead of proactively adding features and functionality that improve employees' experiences and productivity.

Employees want easier ways to get their devices set up, connected, and running. They also demand seamless, easy access to the information that they need when they need it, and self-service capabilities that let them customize their experience and adapt technologies to their work style. Enter Microsoft Surface modern endpoint management solutions, designed from chip to cloud to meet all of these needs and more, while improving IT efficiency and reducing associated risks.

One study found that Surface with Microsoft 365 drives improvement in IT costs related to device management worth $1.4 million.[2]

02.

Increase efficiency with streamlined device management

Surface works seamlessly with Microsoft 365, with built-in UEM capabilities that simplify IT tasks, offer a comprehensive view across endpoints, and enable employees to more effectively manage policies, applications, and updates. Surface also streamlines management of the entire device lifecycle, from deployment and provisioning through to device end of life. That starts before the device is even deployed, with Device Firmware Configuration Interface (DFCI) profiles built into Microsoft Intune, extending Surface Unified Extensible Firmware Interface (UEFI) management of the modern management stack down to the UEFI hardware level.[3] DFCI supports zero-touch provisioning, eliminates BIOS passwords, and gives you control over security settings, including boot options and built-in peripherals, increasing your security now while laying the groundwork for advanced security scenarios still to come.

When a new device is enrolled into your Microsoft Azure Active Directory environment, the profiles you've established—including applications, policies, settings, and more—help ensure that every employee starts their machine up with the correct settings and all of the applications they need immediately available. That helps maximize productivity and delivers a great experience.

03.

Simplify endpoint management and reduce risks

Now you can bring modern UEM to your organization with Microsoft Endpoint Manager while keeping your data more secure, whether in the cloud or on premises.

Endpoint Manager gives you the services and tools you need to manage and monitor mobile devices, desktop computers, virtual machines (VMs), embedded devices, and servers. By combining services that you might already be using as part of the Microsoft 365 stack—including Microsoft Intune, Microsoft Configuration Manager, Desktop Analytics, Windows Autopilot, and co-management—you can better secure access, protect data, and respond to and manage risks. The box to the right describes the benefits of each of these services.

Microsoft Endpoint Manager components

- **Microsoft Intune:** Microsoft Intune helps you let your people use the devices and applications they love while configuring device settings to meet compliance needs. Microsoft Intune also lets you flexibly manage your devices from the cloud or while connected to an existing Configuration Manager infrastructure.

- **Configuration Manager:** Configuration Manager helps you with system-management activities by enabling the secure and scalable deployment of applications, software updates, and operating systems. You can also take real-time actions on managed devices while accessing cloud-powered analytics and management for on-premises and internet-based devices. Configuration Manager even lets you manage compliance settings, and it gives you comprehensive management of servers, desktops, and laptops.

- **Desktop Analytics:** Desktop Analytics is a cloud-based service that integrates with Configuration Manager. With Desktop Analytics, you get the insights and intelligence you need to make more informed decisions about the update readiness of your Windows clients.

- **Windows Autopilot:** Windows Autopilot is a collection of technologies you can use to set up and preconfigure new devices to get them ready for productive use. Windows Autopilot also lets you reset, repurpose, and recover devices while requiring little to no infrastructure to manage using a process that's easy and simple.

- **Co-management:** Co-management lets you concurrently manage Windows devices by using both Configuration Manager and Microsoft Intune. Co-management lets you cloud-attach your existing investment in Configuration Manager by adding new functionality while also giving you the flexibility to use the technology solution that works best for your organization.

Consider a modern device management approach from Microsoft with **cloud-based deployment on Windows devices.**

Azure Active Directory

Azure Active Directory (Azure AD) protects your business with a universal identity platform. With Azure AD, your employees get simple, single sign-on for seamless access to all of their apps, onsite or remotely, so that they can stay productive anywhere. Conditional access and multifactor authentication add another layer of security, protecting and governing access. And with Azure AD, you get a single identity platform that lets you engage with internal and external users more securely. Azure AD also lets you automate workflows for user lifecycles and provisioning, saving time and resources with self-service management. It also includes development tools that make it easy to integrate identity into your apps and services.

Microsoft Surface

Surface device deployment and management solutions powered by Microsoft 365 can increase IT efficiency and reduce IT costs. Surface also minimizes downtime for IT with secure devices that offer efficient, zero-touch device deployments, eliminating time-consuming re-imaging and allowing the device to be shipped straight to your employees. And Surface ensures more efficient, zero-touch device deployments, eliminating time-consuming re-imaging, with the device shipped straight to your employees. Surface even lets you manage devices down to the firmware layer and up through the cloud for an extra level of control when you need it—disabling webcams in high-security settings, for example.

04.

Improve value with modern endpoint management

Microsoft Surface devices can deliver added benefits to your business . According to a Forrester Consulting Total Economic Impact (TEI) study, the potential return on investment (ROI) that enterprises can realize by implementing Microsoft 365 Enterprise on Microsoft Surface devices is notable, especially for IT teams.

Value for IT

Deploying Microsoft Surface devices offer the potential to save time and reduce complexity so your employees can get the technology they need set up and running quickly.

4 hours saved with each device deployed
With Microsoft Autopilot and Microsoft Endpoint Manager, IT departments saved four hours for each device deployed.[2]

67% reduction in help-desk support
IT help-desk call times decreased on average from 45 minutes to 15 minutes with Surface device deployments powered by Microsoft 365.[2]

3.25 hours saved deploying updates on Surface
IT teams faced fewer deployment challenges when Windows Update pushed patches to Surface devices powered by Microsoft 365.[2]

Value for everyone

Microsoft 365 Enterprise on Microsoft Surface devices also have the potential to deliver value across your entire organization.

21% acceleration in business decision making
With real-time access and collaboration, leaders substantially reduced decision-making time.[2]

20% reduction in security breaches
Firms were able to reduce the number of security breaches they experienced annually by about 20 percent for Surface device users.[2]

80% reduction in security-breach remediation costs
Using two-factor authentication and Advanced Threat Analytics, breach-remediation costs were reduced or eliminated using Surface devices powered by Microsoft 365.[2]

05.

Making the move to modern

Transitioning to modern endpoint management has its challenges. Existing IT investments and legacy IT processes and hardware can be some of the biggest roadblocks. Surface removes those roadblocks by delivering value at every step in the modernization process, and it integrates with the Microsoft 365 security stack, which helps detect vulnerabilities and automatically protects your devices at all times. And every Surface component, from firmware to Windows policy settings, is simple to manage. Surface even includes tools that can automatically fix issues, help with troubleshooting, and optimize functionality from brightness controls to battery usage. Microsoft has also built many innovative management features into Windows. But, if your device manufacturer doesn't take advantage of these capabilities, you can't realize the full potential of modern UEM. Microsoft Surface devices offer modern hardware and software that is built to take advantage of the management capabilities of Windows.

When you add it all up, it's clear: modern endpoint and device management with Microsoft Surface can help your enterprise support hybrid and remote workers while delivering multiple layers of security, simplifying IT tasks, and improving your employees' experience.

It's time to make device and endpoint management efficient, simple, and cost effective. It's time to make the move to modern endpoint management with Microsoft.

Simplify device deployment and endpoint management

Learn more about modern endpoint management with Surface for Business.

Contact us today.

[1] IDG. "2020 Security Priorities Study." November 2020. www.idg.com/tools-for-marketers/2020-security-priorities-study/.
[2] Forrester Consulting. "Maximizing Your ROI From Microsoft 365 Enterprise With Microsoft Surface." Total Economic Impact study commissioned by Microsoft. July 2020. https://docs.microsoft.com/en-us/surface/forrester-tei-study.
[3] Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. Find out more about managing Surface UEFI settings.

Microsoft Surface