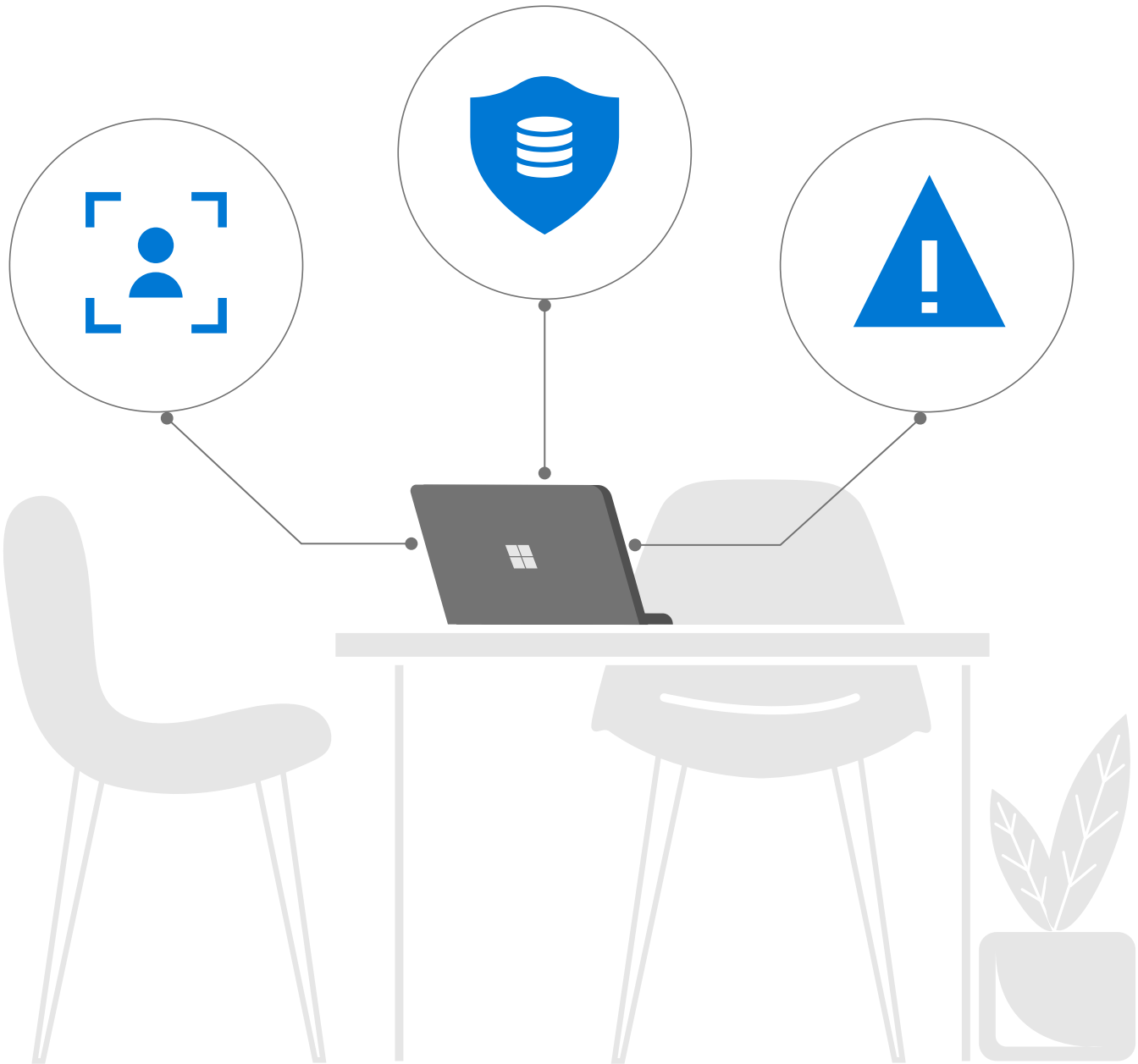
Microsoft Surface

Three ways to reduce the endpoint security risks of a remote workforce



Introduction

Supporting a remote workforce is a lesson in proper balance: you need to make it easy for workers to do their jobs from any location while simultaneously protecting systems and data from known and unknown threats.

In this paper, we'll explain the benefits of a more flexible and scalable approach to protect employee devices, data, and user identities across a dispersed workforce.

Contents

1. Managing and securing remote devices

2. Protecting company information

3. Securing identities

Managing and securing remote devices

Overview

Protecting sensitive information on endpoint devices has typically involved a lot of manual configuration. These tasks become more impractical with a workforce dispersed among many different locations.

Many organizations are opting, therefore, to move to cloud-based solutions that combine device protection, information protection, and identity protection. Cloud-based mobile device management (MDM) eliminates bottlenecks and ensures that the software and operating systems on your devices are always up to date.

—

Microsoft has pioneered a "**zero-touch**" deployment approach for Surface and other Windows 10 devices that leverages services such as Windows Autopilot and Intune to allow secure configuration and delivery of devices to users without the IT team ever physically touching the computer.

This automated, hands-off approach reduces the time to get a new device up and running from hours to minutes. What's more, Microsoft harvests the Device ID of each Surface sold and stores it in the cloud for device management.

Device considerations

Endpoint security begins with the design of the device and continues throughout the entire device lifecycle, from deployment to end of life. An optimal security strategy enables administrators to control even the lowest level of hardware settings without having to touch the machine.

—

Unified Extensible Firmware Interface (UEFI) is a standard for booting devices and loading the operating system. Most manufacturers buy a UEFI from a third-party vendor, which provides updates to the manufacturer, which in turn distributes these updates to customers.

The UEFI* in Surface devices, by comparison, was written by Microsoft, so updates to it are pushed to the customer automatically through Windows Update for Business rather than having to be manually pulled by IT and packaged for delivery to users. This makes updates not only timelier, but also more likely to be applied.

Scenario 1: Deploying a new device

Natalie has been issued a new Surface Book 3, which was delivered to her home. In the past, IT would have manually configured a device before deployment with a custom software image and the settings required to allow Natalie to connect to the corporate network. After receiving the new device, Natalie would log in, then have to follow a series of time-consuming tasks to finalize set-up before she could access her work apps and services.

But now:

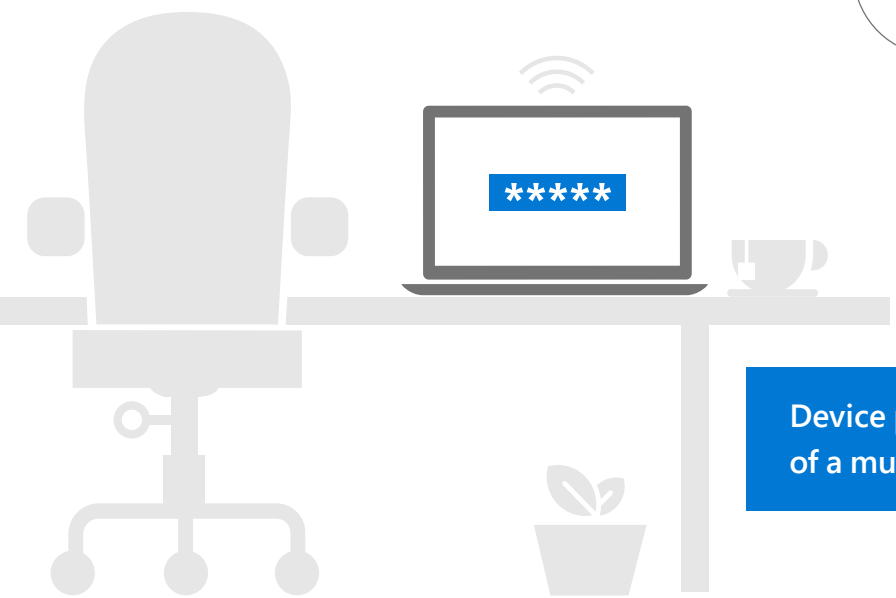
When Natalie turns on her Surface Book 3, Autopilot delivers a customized set-up experience based on the profile assigned to her device.

The first time she signs into her email, Natalie is instructed to enroll in Microsoft Intune.

She authorizes the device to be managed by Intune, and all the relevant IT policies, apps, and settings are applied automatically—with no risk of user error.

Natalie doesn't need to bring the device to IT to be configured manually—it can all be done automatically.

Intune also integrates with the company's Azure Active Directory domain, so Natalie has access to all relevant business applications and data without having to create an additional user ID and password.



Device protection is a foundational component of a multi-layered approach to security.

Protecting company information

Overview

Protecting your company's information from loss, theft, and misuse becomes more critical—and more complex—with a dispersed workforce.

For many organizations, the best way to remain compliant with data privacy and other regulations is with a cloud-based solution that can help you classify and protect information regardless of where it's stored or who it's shared with. A modern information protection solution can automatically discover information as it appears, apply custom controls based on how it is classified, and apply policy-based actions to sensitive information.

—

Azure Information Protection lets you classify, label, and protect data based on its sensitivity. You can use the service to ensure that sensitive data such as Social Security numbers, birthdates, addresses, and credit card information is properly labeled and classified. Azure Information Protection can classify the data automatically or based on user recommendations.

Device considerations

Alongside a cloud solution for information protection, the devices you choose also play a big part in protecting sensitive data.

For example, modern biometric login solutions offer better protection than passwords, by using fingerprint and facial recognition. Plus, some devices offer instant and built-in data encryption, without the need for additional configuration by IT, so information on the hard drive can't be accessed if the device is lost or stolen.

—

Surface Pro, Laptop, and Book devices includes a **Trusted Platform Module** (TPM) chip that makes it fast and easy to authenticate devices and encrypt data. The TPM chip works with BitLocker encryption in Windows 10 to protect data from unauthorized access.

Scenario 2: Keeping remote data secure

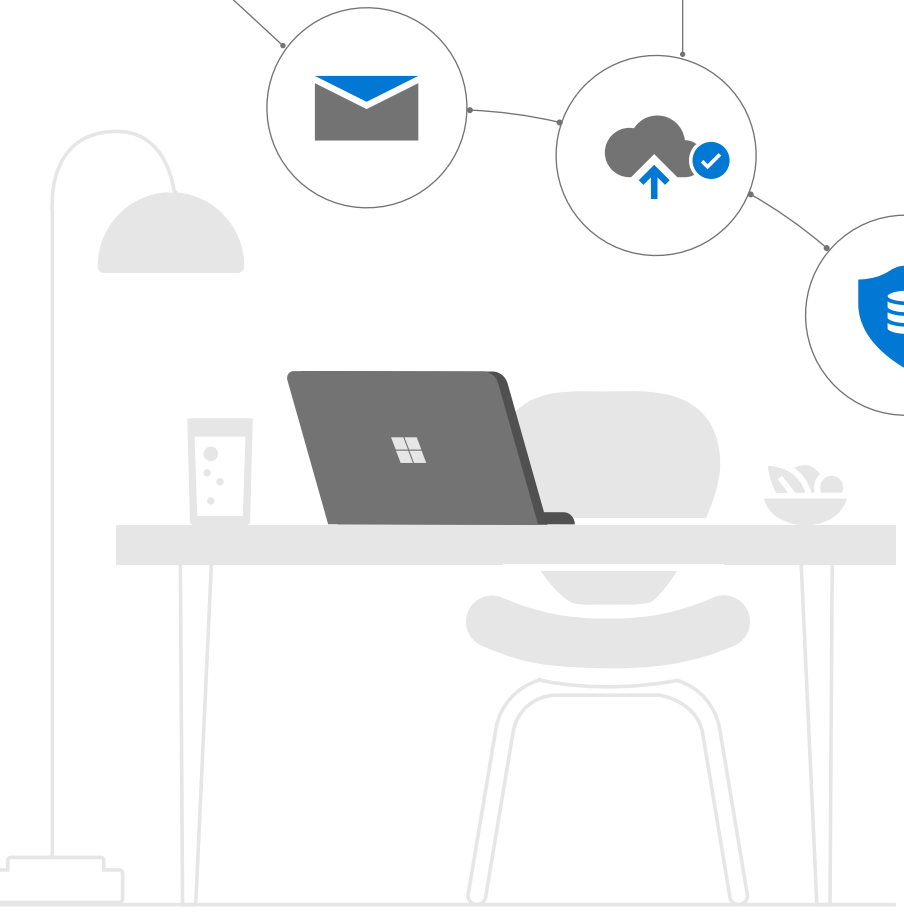
Anna has been set up with remote access to her work through Exchange Online, but often receives confidential information that could present a risk if lost or stolen.

With the right remote access system in place via Windows Virtual Desktop, that information can only be accessed via managed apps on her device—removing any security blind spots.

Emails can't be copied into personal apps by mistake or posted to social media.

If files are encrypted, Anna's software can't open them without first contacting the cloud service to check her identity and determine what access rights she has.

Policies can also be applied to detect sensitive data (such as credit card information) and automatically apply protection (such as Do Not Forward).



Cloud-based security enables organizations to protect exposure of sensitive information in transit and at rest, using automated processes to apply controls in real-time across all of your cloud apps.

Securing identities

Overview

Many businesses have adopted a single sign-on (SSO) solution that lets users access multiple applications with just one credential. Consolidating logins to a single set of credentials improves security by reducing the attack surface (the more passwords used, the greater the opportunity for attackers to exploit weak passwords).

However, as the popularity of cloud applications grows, relying solely on an on-site SSO is no longer enough. Creating a direct connection each time between your SSO solution and every single cloud application, for every single user, is far too complex to manage. A simpler approach is to use a cloud solution for identity management.

Single-point identity confirmation is no longer enough either. Multi-factor authentication is more secure—and it needn't be a burden for the organization or its users.

—

Windows Hello for Business let you replace your passwords with strong two-factor authentication (2FA) on Surface and other Windows 10 PCs. Use a credential tied to your device along with a PIN, a fingerprint, or facial recognition to protect your accounts.

Device considerations

In addition to the convenience that SSO brings to how people work, there are new hardware technologies that help drive identity-based security. For example, Surface devices are configured out of the box with "containers" that isolate apps from other processes to protect them from misuse.

Choosing hardware that supports these new methods—in combination with cloud-based identity management—will help you build a strong defense against today's growing threats.

For instance, devices are increasingly available with fingerprint or retina-scan authentication in addition to traditional passcodes, as well as out-of-the-box software that isolates and hardens key system and user secrets against compromise.

—

Fast Identity Online (FIDO) is an open standard for passwordless authentication. Users of Windows 10 devices can use FIDO2 security keys, in the form of an external security key or a platform key built into a device, to sign on to their Azure AD or hybrid Azure AD joined devices and get single sign-on to their cloud and on-premises resources. Users can also sign in to supported browsers. FIDO2 security keys are a great option for enterprises who are very security-sensitive or have employees who may be unwilling or unable to use their phone as a second factor.

Scenario 3: When a threat occurs

Chris has chosen an easy-to-guess password and a hacker has assumed his identity, putting valuable business data and resources at risk. Previously, this would have been a significant security blind spot.

However:

With identity-driven security, staff will be warned about risks proactively, as soon as suspicious activity occurs.

If "Chris" signs into his account from Germany, then five minutes later signs in from the U.S., suspicious activity will be flagged.

Similarly, if a device type using Chris's identity is different than what Chris normally uses—or if the device is infected with malware—staff will be notified.

Advanced solutions can also detect unusual activity by analyzing SSO traffic and learning what a typical day looks like for Chris, so if he starts accessing atypical apps and data, an alert will be raised.

Using Windows Hello, IT can replace passwords altogether with strong two-factor authentication using a biometric or PIN.

Identity management is a critical component of advanced security models such as the Zero Trust security architecture.

Microsoft Surface

Conclusion

Secure from chip to cloud

With the proliferation of remote work, employees need consistent access to their familiar work tools and data on whichever device they're using, so they can be just as productive in the home office as they would be in the corporate office.

Endpoint devices that are built with security in mind help IT and security leaders enable the benefits of working remotely while ensuring that their business data and IP is protected from unauthorized access.

Security protections maintained by Microsoft are built into every layer of Surface. Learn more about how Surface is the right choice for organizations looking to build and maintain productivity and secure remote work environments.

Find a reseller

*Surface Go and Surface Go 2 use a third-party UEFI and do not support DFCI. DFCI is currently available for Surface Book 3, Surface Laptop 3, Surface Pro 7, and Surface Pro X. Find out more about managing Surface UEFI settings.