Microsoft

The security challenge in a mobile world

Contents

Executive summary

As organizations increase their mobility and cloud footprint, they're also grappling with ensuring their people and customers remain secure from any location. Of course, there is no single answer, but there are steps that can be taken, such as making use of the latest mobile device management (MDM) solutions, biometric security, and using modern business devices that have been built expressly for mobile workers.

As more mobile devices are deployed, increasing numbers of blindspots are revealed. New applications are more likely to be accessed as-a-service, rather than being installed on site, which in turn creates new challenges around identity. Furthermore, cyber-attacks are becoming more sophisticated, requiring better protection over company data and IP.

IT leaders across all industries are recognizing the limitations of their legacy on-site security setups, and are seeking new ways to meet today's modern challenges while addressing annual budget restrictions.

In this paper, we'll consider why blending on-site security with MDM will give you a more flexible and scalable way to secure your mobile devices, data, and user identities.

We'll also outline some key considerations when investing in new mobile devices, so your business gets the full benefits of the latest trends in IT.

Plus, we'll explore some typical workplace scenarios to show how this results in practical benefits for your people and your business.

Security wish-list

- For mobile staff to safely access the tools and data they need, across devices and on the move.
- For business devices, data, and IP to be protected against new and changing cybersecurity attacks.
- For security updates and new features to be applied quickly and easily across a fleet of devices, so everyone is up to date.

Controlling devices and data from the cloud

A big challenge for IT decision-makers is how to respond to major technology shifts in a way that both benefits and protects the business.

Prior to the move to mobility and apps, IT security issues were contained within the network perimeter and easy to lock down and control.

But now there are added layers of complexity:

- Devices are more diverse and often outside your network perimeter.
- Information can reside outside the perimeter on devices and in the cloud.
- Attacks are growing more sophisticated (as this infographic clearly shows)

In response, many businesses are turning to a hybrid approach that blends on-site systems with security technologies hosted in the cloud.

Over the following pages, we'll explore why cloud-based management of devices, information, and users is so important and what benefits you could expect for your business.

Managing mobile devices

Overview

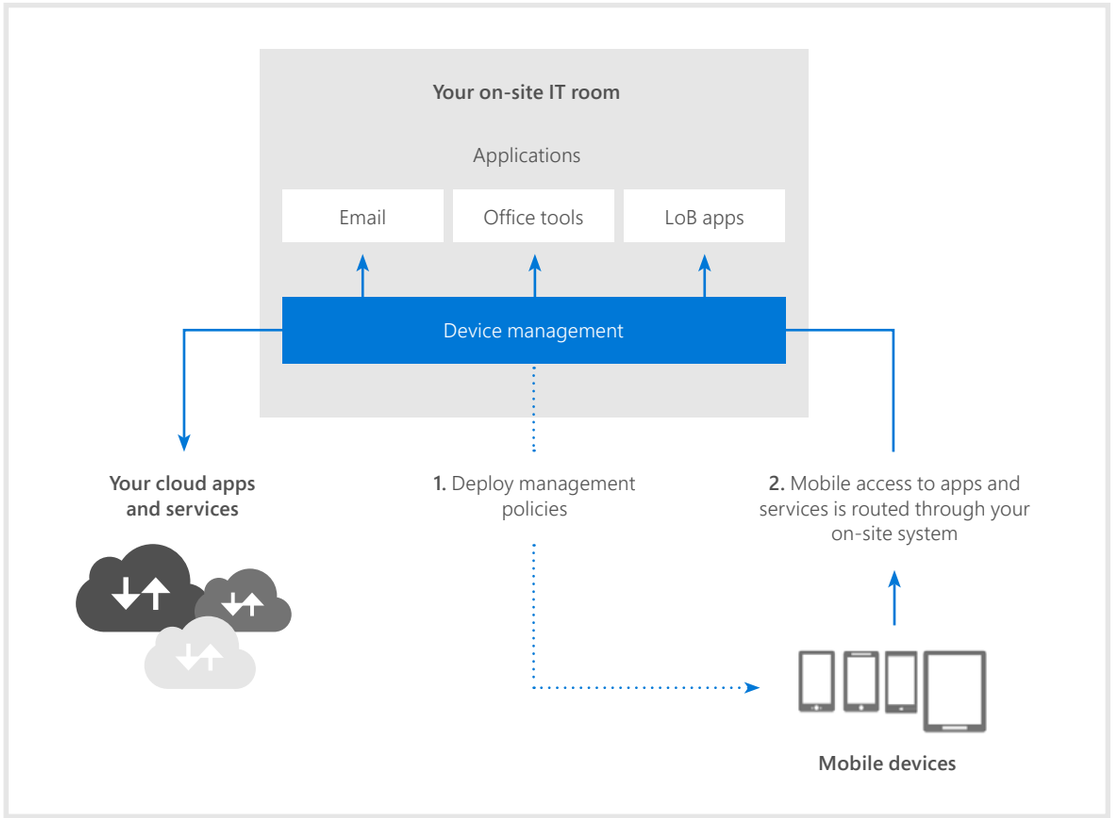
As mobile working becomes integral to all businesses, employees, devices and applications have become the front line of defense.

On-site management and security solutions were perfect when mobile devices were only accessing commercial data from within the corporate network.

But with data going mobile, it no longer makes sense for communications to be routed through an on-site solution. It just creates a bottleneck. Requests will be flowing from mobile device to on-site server to mobile app, then back to the server and back out to the device. The speed of interaction between device and applications will be limited to what your on-site management solution can handle.

Plus, as you equip more staff with mobile devices and move more applications to the cloud, you will only have to add more capacity and commit more resources to support it.

Which is why a cloud-based solution makes more sense.



Managing mobile devices

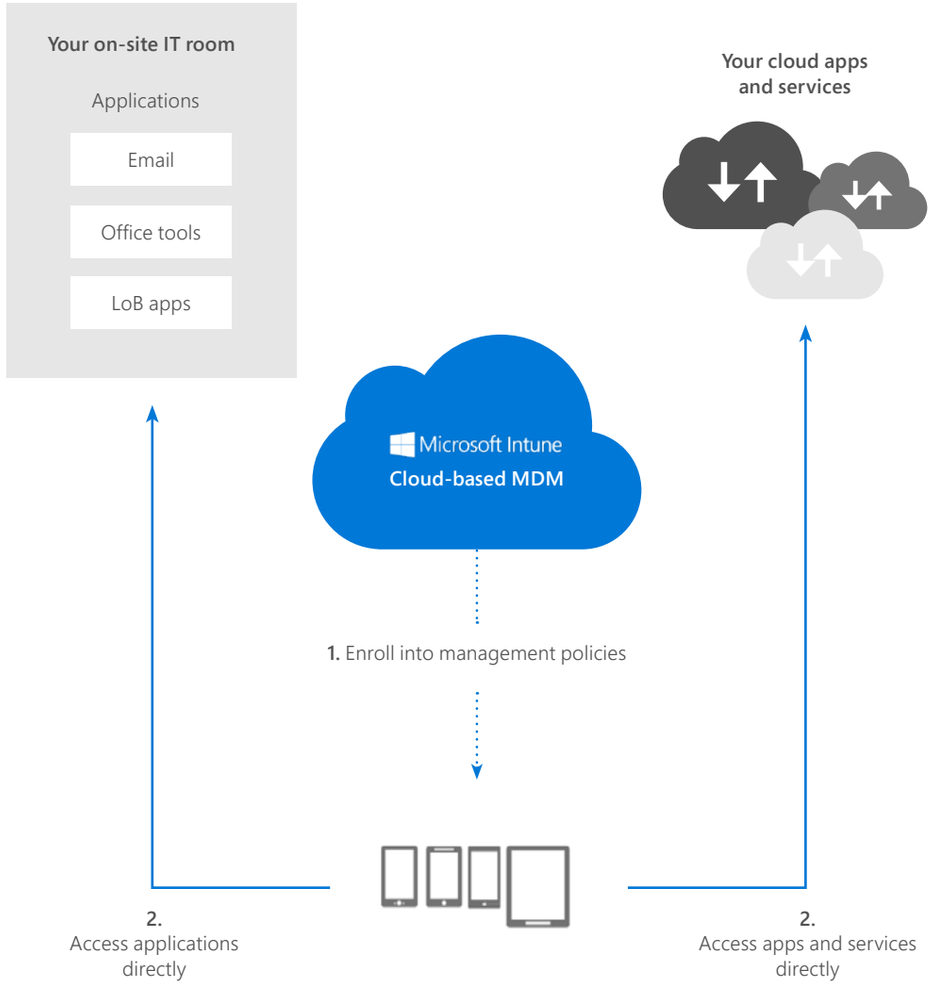
How it works with MDM

Mobile devices receive policies from a mobile device management (MDM) solution. Once these policies are in place, the devices can communicate directly with both on-site applications and cloud-based applications. The on-site bottleneck is gone.

A cloud-based MDM solution has other benefits too, like keeping the software and operating systems on your devices up to date. Microsoft Intune is a cloud-based MDM solution. For the sake of this document, the examples will use Intune as the solution. There are third-party MDM solutions which may also address these scenarios.

With on-site solutions, you often need to wait for the vendor to ship the updates to you, which takes time, before then testing them and then rolling them out to your devices. Multiply this by the number of different operating systems you're supporting, and the result is clear: you'll probably never be current.

But with MDM in the cloud, this problem goes away. When a new release is rolled out, the system updates itself to support whatever changes this update brings. You're always up to date, and you never need to worry about installing updates.



Managing mobile devices

Scenario 1:

Deploying a new device

Natalie has been issued a new mobile device. It needs to be connected to the corporate network and configured to access her work apps and services. In the past, this would have been a blindspot for IT, with Natalie attempting to log in manually.

But now:

- The first time she signs in to her email, she is instructed to enroll into Microsoft Intune.
- She authorizes the device to be managed by Intune, and all the relevant IT policies are applied automatically—with no risk of user error.
- Natalie doesn't need to bring the device in to be configured manually—it can all be done automatically.
- Intune also integrates with the company's Azure Active Directory domain so Natalie has the relevant access to her business applications and data without having an additional user ID and password.

Protecting company information

Having control over who can access specific business information—including the level of access they are allowed—has always been important.

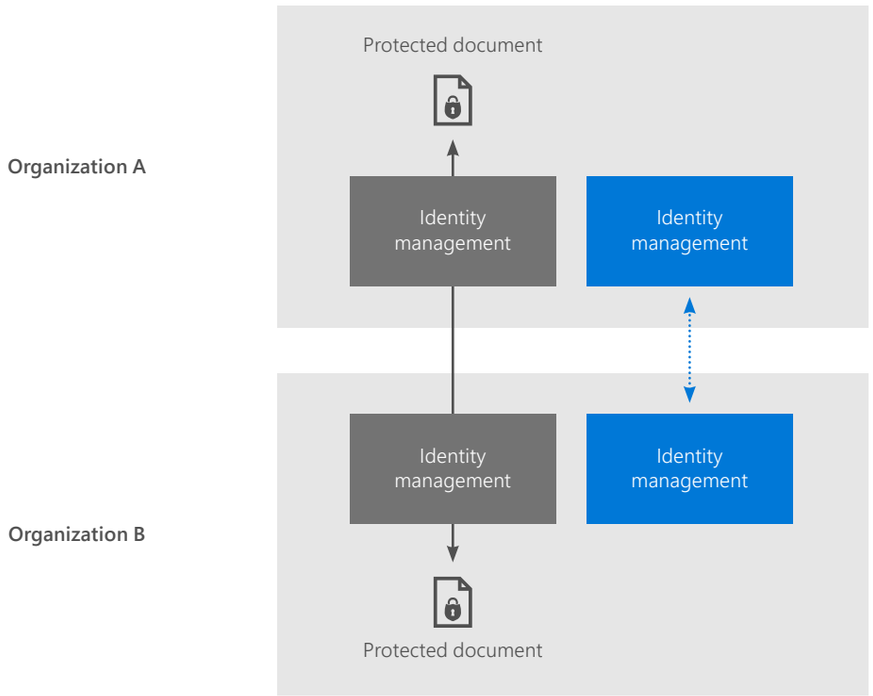
Making sure that data and IP is properly protected, right from the point of its creation through to the different ways it is accessed and used during its lifecycle, is a critical requirement of most IT functions.

However, this has typically involved a lot of manual configuration.

Providing secure file access to specific people in different organizations requires a system that verifies each request to open that file. Which means manually linking together separate file storage and identity management solutions.

For many businesses, this level of configuration isn't often practical or realistic. And as we've already seen with device management, the recent boom in mobile devices and demand for secure remote file access makes it even more complex.

Many organizations are therefore choosing a shared cloud solution for information protection. They're also looking at out-of-the-box device encryption.



Typical approach to providing secure file access across organizations

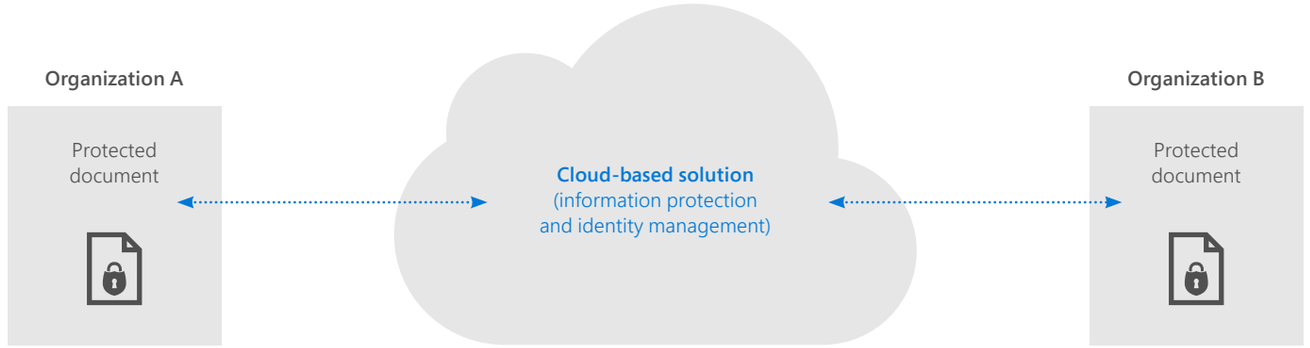
Protecting company information

The benefits of a shared cloud / encrypted device approach

If two organizations want to share information securely, they no longer have to set up direct connections to each other. Instead, they simply connect to a single cloud service, which verifies their identity and authorizes access to the required information.

No matter how many other companies you want to share documents with, you only ever need to connect once to the cloud service—removing the traditional complexities of sharing protected documents.

What's more, the devices on which company information may be held can also be protected with encryption out-of-the-box using Trusted Platform Module (TPM) technology. This approach offers a single sign-on (SSO) procedure and is easy to deploy, creating no work for the IT team.



A shared cloud solution greatly simplifies the sharing of protected documents between different businesses.

Protecting company information

Device consideration

As people choose (and demand) to work more on the move, protecting your company's information from loss, theft, and misuse is increasingly important.

As we've seen, alongside a cloud solution for information protection, the devices you choose can play a big part in this too.

For example, modern biometric log-in solutions offer better protection than passwords, 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 stolen.

Scenario 2:

Keeping data secure on the move

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

With the right system in place, that information can only be accessed via managed apps on her device—removing any security blindspots.

- It 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).

Securing your identities

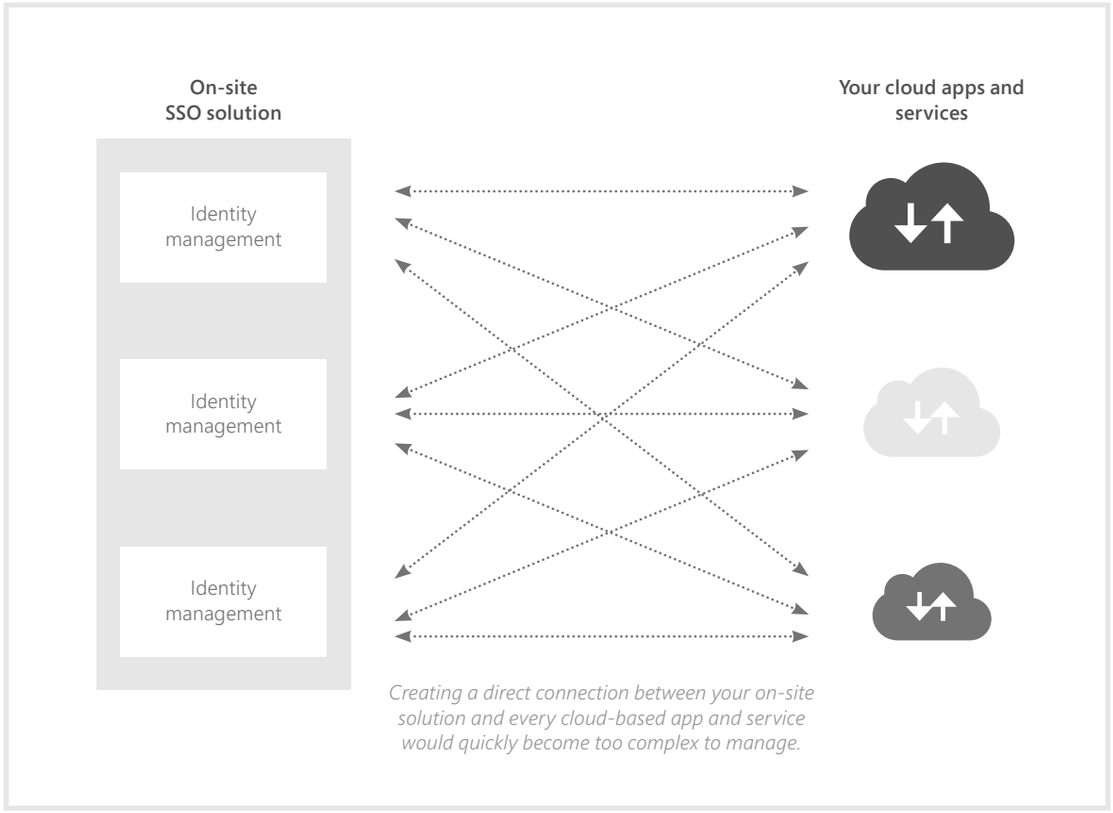
The idea that individuals will use a different password for individual sign-ins is unlikely. And that makes passwords a risk. It's also why many businesses have adopted a single sign-on (SSO) solution that lets users access multiple applications with just one credential.

A typical on-site SSO solution makes direct connections to the applications that users want to access, and logs them in automatically. Which is fine if those applications are all running on site too. But if they are hosted in the cloud, problems quickly arise.

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—and puts far too much strain on the network.

So as the popularity of cloud applications grows, relying solely on an on-site SSO is no longer enough. 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.



Creating a direct connection between your on-site solution and every cloud-based app and service would quickly become too complex to manage.

Securing your identities

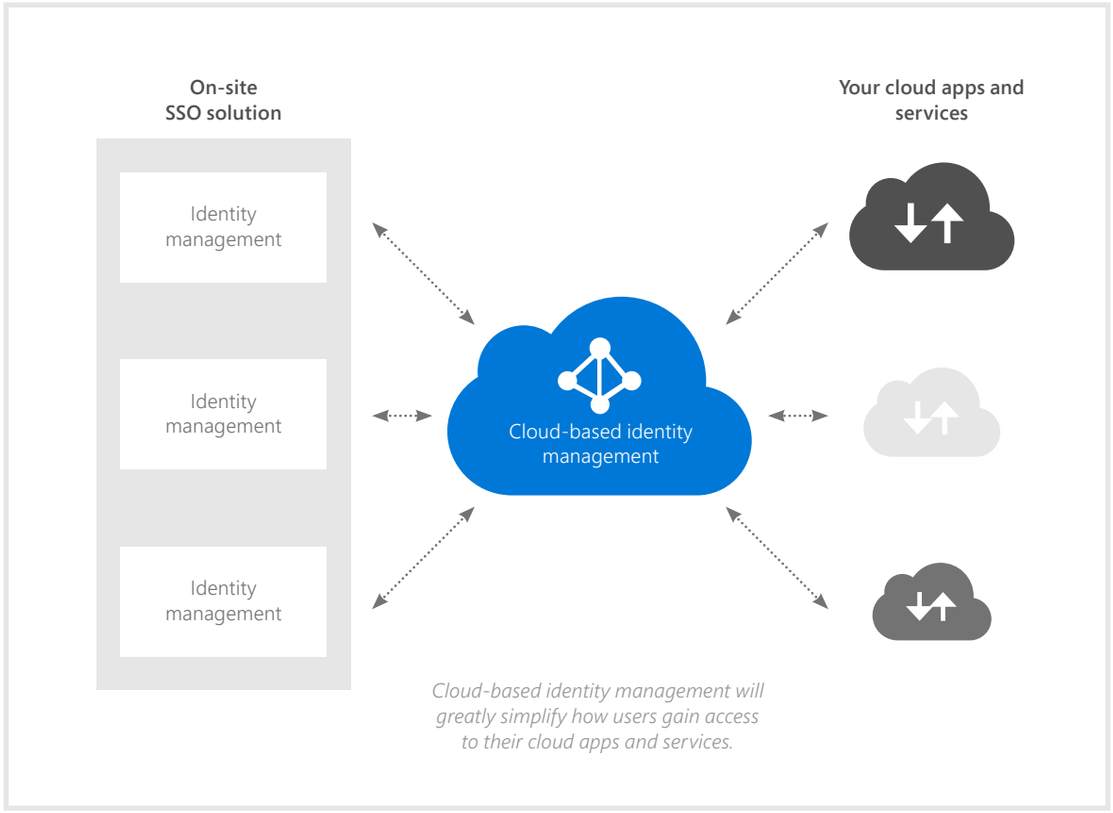
Why it works better with the cloud—and with device-level authentication

Put simply, your on-site SSO solution is linked to a directory service in the cloud, which then makes connections to your cloud-based applications.

You retain control over your users' identities, as they all still come from your own directory service. However, by exploiting the power of the cloud, you've given them easy access to both local and cloud-based applications with a single sign-on. You've made life better for your users and simpler for your organization.

Of course, having security over your cloud apps and data doesn't make securing your on-site environment any less important. So this should be complemented with a modern threat analysis solution that helps you identify suspicious activities before they cause damage.

It should also be complemented by device-level authentication—ideally offering a single sign-on (SSO) and multi-factor approach specific to the biometrics of individual users.



Cloud-based identity management will greatly simplify how users gain access to their cloud apps and services.

Securing your identities

Device consideration

In addition to the convenience that SSO brings to how people work, there are also new hardware technologies that help drive identity-based security.

Some devices are also configured out of the box with ‘containers’ that isolate apps from other processes to protect them from misuse.

So, 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.

Scenario 3:

When a threat occurs

Chris has chosen a guessable password and a hacker has assumed his identity, putting valuable business data and resources at risk. Previously, this would have been a significant security blindspot. 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 US, suspicious activity will be flagged.
- Similarly, if a different device type is being used to 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.

Conclusion

With the proliferation of mobile devices in the workplace, employees are now working from just about anywhere. To stay productive, they demand consistent access to their familiar work tools and data on these devices, so they can be just as effective as they would be in the office.

This trend has introduced significant challenges for IT and security leaders who want to foster all the benefits of working remotely, while ensuring that their business data and IP is protected from unauthorized access.

Coupled with the trend toward cloud collaboration and software-as-a-service, it's fast becoming apparent that on-site security solutions alone do not have the capacity to provide the assurance that businesses need today.

Businesses should be looking at a hybrid approach that supplements their existing on-site systems with cloud-based control over devices, information, and user identities.

Here is some useful, practical guidance on how to design a Mobile Device Management solution that's right for your business.

Alongside MDM, you should also be considering all future IT investments in the context of this. For example, any new hardware you purchase should be:

- Easy to integrate with existing on-site ecosystems.
- Fully compatible with MDM and cloud-based SSO solutions.
- Designed for protection against increasing threats to data and identity.

Find out why we believe Microsoft Surface are the perfect devices for organizations looking to take advantage of mobility, while retaining security and control over their IT.

Alongside the importance of security, we know that you're always striving to get the very best out of your people too.

So in our next paper, we look at how Surface, together with Windows 10 and Office 365, is helping businesses be more creative, collaborative, and mobile in order to maximize the value of their ideas.