NEXINITE

How InTune Secures Data and Devices

For a Workforce in the Office and at Home

A Whitepaper By Nexinite

Table of Contents

How InTune Secures Data

The Current State of Work

1

The Current State of Work

The COVID-19 pandemic made lasting changes on how people work.

For example, businesses scrambled to make remote working a viable option for as many employees as possible. And with less people accessing data at the office, companies worked to protect their devices and make their data less vulnerable to breaches.

This white paper explores how InTune, a Microsoft cloud-based service with a focus on data security, is an ideal solution for the current state of work.

REMOTE WORK IS HERE TO STAY.

73%

OF WORKERS WANT MOBILE OPTIONS TO CONTINUE.

In Microsoft's 2021 Work Trend Index Annual Report, researchers found that 73% of the workers surveyed want mobile work options to continue. Yet, researchers noted that 67% of those participants want more in-person opportunities with their coworkers post pandemic.

This large study, which included over 30,000 participants from 31 global markets, confirms what you have known for a while - remote work is here to stay for many industries.

+33%

OF COMPANIES HAVE REPORTED DATA BREACHES DUE TO MOBILE WORKERS.

And workers want a hybrid option, one that allows them to work from home and at the office.

SECURITY CONCERNS.

90%

OF IT LEADERS FEEL TELEWORKING JEOPARDIZES SECURITY.

Remote working, although beneficial during the pandemic, has its drawbacks. The security of company data and devices is an obvious one.

A recent study by OpenVPN found that over a third of companies reported data breaches due to mobile workers.

And of the 250 IT leaders surveyed for this study, 90% feel teleworking jeopardizes security. So, if vulnerability of devices and data worry you, you're not alone. It's a valid concern.

Why InTune

2

Why Microsoft InTune

There are lots of partial solutions for making devices and data more secure for the remote work environment. More training for employees at all levels, updated policies and strict adherence to procedures are three of the best ways. InTune by Microsoft can help bring these solutions to fruition.

WHAT IS INTUNE?

InTune is a cloud-based service by Microsoft that makes mobile device management (MDM) and mobile application management (MAM) much easier and quicker.

InTune helps you control how data is used on devices, push out policies and compliance requirements to devices remotely and regulate how applications are used on company-owned and personal devices.

Also note, InTune is a part of Microsoft's Enterprise + Mobility Suite (EMS). It integrates with Azure Active Directory (AD) and can be used with all Microsoft 365 products. If you're not completely cloud based, that's no problem. With InTune, you can opt to be co-managed using Configuration Manager.

DEVICE MANAGEMENT.

InTune helps you manage both company-owned and personal devices. With bring your own devices (BYOD) initiatives growing in popularity, this InTune feature is a significant one. With InTune, administrators can...

- Separate company data from personal data
- Employ multi-factor authentication (MFA) to give employees using personal-owned devices access to apps like Teams or email
- View reports about compliant and noncompliant devices and users
- Delete company data if a device is lost, stolen, or no longer in use

APP MANAGEMENT.

InTune manages data at the application level. This includes store apps, as well as custom apps. With InTune, administrators can...

- Control how users access apps to secure company data
- Remove only company data from an app
- View how apps are being used

How InTune is Being Used

3

How InTune is Being Used

In a February 2021 memo, Microsoft engineers outlined 6 of the most common ways InTune is being used to make workforces more mobile WHILE more secure.

If you're not already employing InTune, these scenarios may provide context for how your organization can use it.

1. **Secure on-premises email so it can be safely accessed on mobile devices**

2. **Protect Microsoft 365 data and email to ensure secure access by mobile devices**

3. **Allow bring your own device (BYOD) policies for all employees**

4. **Issue company-owned phones to workers**

5. **Provide limit-use shared devices to employees**

6. **Allow workers to access Microsoft 365 using public, unmanaged devices (example: computers in hotel lobbies)**

Conclusion

In many industries, remote work to some extent is here to stay. So the next step is to ensure the security of your organization's data and devices as people work at the office and from home.

InTune is a cloud-based service by Microsoft that provides MDM and MAM. This means you control how your company's devices and any applications downloaded to them are used. And because of InTune, bring your own device (BYOD) is now a viable option in many organizations.

InTune is an ideal security solution for the post pandemic work environment.

What questions do you have about how InTune can help you and your company? We'd be glad to answer them.

Contact us here so we can schedule a call with each other.

Whitepaper References

Microsoft. (2020, June 23). Microsoft InTune is an MDM and MAM provider for your devices. https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft. (2021, February 4). Common ways to use Microsoft InTune. https://docs.microsoft.com/en-us/mem/intune/fundamentals/common-scenarios

Microsoft. (2021, March 22). 2021 Work Trend Index: Annual Report. https://www.microsoft.com/en-us/worklab/work-trend-index/hybrid-work

Open VPN. Remote work is the future – but is your organization ready for it. https://openvpn.net/remote-workforce-cybersecurity-quick-poll/