BYOD security:

An exhaustive approach with UEM

WHITE PAPER

hexnode

Table of Contents

Introduction

The Bring Your Own Device scenario, usually known by its acronym BYOD, relates to the notion of organizations and enterprises enabling the workforce to carry their own high-end mobile computing devices into the workplace for personal as well as business purposes. The mobile devices incorporated in a BYOD environment can be smartphones, tablets, personal computers, or USB drives. The employees generally use these devices for accessing work-related systems and potentially sensitive data by connecting to their organizational networks. The BYOD strategy is also referred to as the consumerization of Information Technology due to the influx of consumer software and hardware into the enterprise. Before the advent of BYOD, the employees did not get access to the corporate networks because the Information Technology (IT) department of organizations maintained closed networks that were accessible only to the company-owned devices.

> "The strategy of organizations, making their computer networks available to the workforce, marked the dawn of the BYOD concept."

The BYOD program gained prevalence in the world of enterprise mobility with the rapid proliferation of smartphones, tablets, and low-cost laptop computers. An enterprise mobility environment fastened with a BYOD strategy enhances workplace productivity by allowing the workforce to use

their convenient devices for work. A BYOD strategy can considerably reduce organizational expenses by eliminating the need for purchasing extensive device hardware. Apart from the various benefits, the BYOD scenario also opens the door to potential risks and security vulnerabilities. Therefore, incorporating BYOD within your enterprise won't work well without maintaining a proper management strategy for the BYOD environment. This whitepaper lets you understand the widespread adoption of BYOD, its impact on the current era of enterprise mobility, and the role of Hexnode in building a robust BYOD ecosystem.

The significance of BYOD

In recent years, there has been a steep rise in the use of mobile devices for computing. The rapid advancement in mobile technology was the principal factor that led many companies to implement the BYOD strategy in their workplaces. Seeing that the modern mobile technology offered a lot more security options, BYOD was gradually implemented across enterprises. The BYOD scenario brought about many refined categories such as Bring Your Own Technology (BYOT), Bring Your Own Computer (BYOC), Bring Your Own Laptop (BYOL), Bring Your Own Apps (BYOA) and Bring Your Own PC (BYOPC) to fit specific use cases in different organizations. The Bring Your Own Technology (BYOT) is a slight variation from BYOD, that relates to a strategy where employees can utilize their own technologies such as Artificial Intelligence-based solutions, event-driven software, web browsers, antivirus applications, and media players within their company.

> "The ability to enhance employee experience while maximizing productivity makes the BYOD program, a signifcant workplace trend in today's competitive business world."

Why is it essential to have a UEM suite alongside your BYOD deployment?

BYOD security is a crucial consideration for IT administrators because the mobile workforce is increasingly expanding and gaining a strong foothold in enterprises today. The implementation of a BYOD plan without a proper management strategy can expose organizations to new security threats and vulnerabilities.

> "The Unified Endpoint Management systems play a vital role in alleviating the BYOD security risks, thereby keeping enterprise data secure. A robust UEM solution enables users to have complete access to personal data while maintaining the tactics to keep all the corporate content under security control."

In a BYOD-deployed corporate network, there are high chances of device loss or theft that can put the confidentiality and security of employee-owned devices at high risks. Most of the UEM systems possess the capability to remotely wipe mobile devices when they happen to fall into fraudulent hands. UEM solutions that isolate corporate data and apps from personal data and apps helps organizations to safeguard their sensitive data against unauthorized access. By keeping corporate and personal content separate on devices, IT admins can ensure that employees can use their devices the way they want while maintaining tight security measures over corporate data and applications.

The benefits of BYOD

The increasing trend of employees bringing their own devices to work can benefit both the employer as well as the employees by making the workspace more open, well organized, and relaxed. Listed below are certain notable benefits reaped from an effective BYOD implementation.

Enhanced productivity

When employees are enabled to utilize their convenient devices in the workplace, organizations can boost their productivity to new heights. By allowing the workforce to use their personal mobile devices, they can deliver prompt responses and comfortably work in their desired environment, thereby improving organizational productivity and creativity.

Cost-effectiveness

With a BYOD program, organizations can considerably reduce their business budgets by eliminating the need to buy each employee specific devices and equipment. Since the workforce brings their personal devices to the workspace, they bear the majority or the entire costs for the mobile devices, data services, and other associated expenses.

Improved work satisfaction

Employee satisfaction is the most crucial factor that leads to high-quality work. The use of personal devices supports the workforce to make the best use of their time through a comfortable and healthy working environment.

Technology utilization

The BYOD devices usually keep up with the continually varying trends in technology. The most modern innovations, capabilities, and upgrades help organizations to gain the upper hand to confront the rapidly-evolving global business environment.

Increased employee engagement

The BYOD strategy can give employees the flexibility to work anytime, anywhere with seamless access to their enterprise applications and data. This leads to a significant increase in employee involvement within the workplace and even outside of it.

Minimized stress on IT

With BYOD implementation, the IT staff need not worry much about the maintenance of mobile devices and hence giving them more time for other essential business processes. The use of personal devices makes employees more alert and responsible for the safety and maintenance of their devices.

Benefits of deploying BYOD over Corporate Owned Personally Enabled (COPE) strategy

BYOD	COPE
- Strategic cost reduction.	- Greater deployment costs.
- Fast and easy deployment.	- Harder implementation due to extensive corporate regulations.
- Serves both personal and business needs.	- Greater restrictions on personal activities.
- The use of familiar devices reduces the learning curve on device operation.	- Requires a steep learning curve in getting acquainted with the technology.
- Allows employees to work remotely with access to all the corporate resources.	- Enable users to access the company resources often only within the corporate network.
- Modern workplace trend that gives employees more freedom and comfort over their work.	- Minimal employee freedom with limited device choice.

The challenges of BYOD

Although BYOD builds a better workplace with enhanced productivity, it can pose severe IT security threats to organizations. The following are some of the potential risks associated with BYOD implementation in the workplace.

Device loss and theft

When the employee-owned devices in an organization are either misplaced or stolen, unwanted third-party individuals attempt to gain access to sensitive corporate content. If the devices are not secured with passwords or passcodes, it becomes effortless for intruders to gain unauthorized access, thereby increasing the frequency of data breaches within the enterprise network.

Access to unsecured Wi-Fi networks

When employees use their devices outside the workplace, there can be chances for the devices to get connected to unsecured public Wi-Fi networks. The network access via unsecured Wi-Fi connection can put their company's data or network at significant risks.

Employees leaving the organization

The IT admins may not get enough time to wipe devices when employees leave their organization abruptly. This leads to a situation where the previous employees get seamless access to enterprise data even after when they are not part of the company anymore.

Insufficiency or absence of firewall and anti-virus software

Anti-Virus software or firewall can help protect mobile devices against viruses and other malware threats. The lack of firewall and anti-virus software in mobile devices may create high chances for the occurrence of security holes within the enterprise networks.

Device disparities

With BYOD, employees connect to corporate networks with a wide variety of devices with diverse capabilities and operating systems. Therefore, all the employees need not necessarily have the latest security provisions on their devices, thereby putting the company's security at risk.

BYOD management with Hexnode

The absence or lack of a proper BYOD management strategy can bring about potential threats to a company's valuable and sensitive data. To minimize the risks of BYOD implementation, businesses must be keenly aware of their exact requirements and goals. Also, the IT admins should take care not to encourage the employees bringing personal devices to the workplace without having a robust security management plan for BYOD.

With capabilities such as remote wipe, data leakage protection, anmore, Hexnode MDM provides efficient methods for protecting business-critical data and other essential corporate assets.

> "Hexnode MDM manages the BYOD deployments of an organization by enabling the IT admins to configure password complexity specifications, device restrictions, network settings, app settings, and other necessary restrictions seamlessly over the air."

Containerization

Containerization organizes separate, encrypted containers on personal devices, thus separating work app and data from personal app and data. Hexnode helps to remotely wipe the container in the event of device loss or theft. With the act of managing only the "container" with work apps and data, Hexnode guarantees that an organization's corporate data never gets merged with any of the employee's personal data.

Android containerization

Hexnode MDM streamlines the management of Android devices in a BYOD environment by deploying Android in the Enterprise Program within the organization. The program manages Android devices either entirely or by creating a separate work container on the devices. If a device needs to be wholly controlled by the organization, then it can enroll in Android in the Enterprise Program as Device Owner. Instead, if the organization wants to manage only the work apps and data, the device can enroll as Profile Owner.

Business Container for iOS

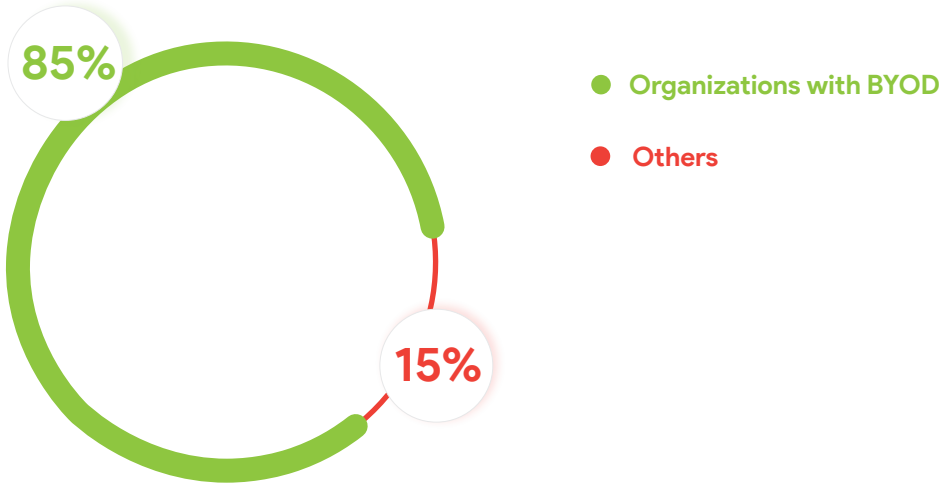
Hexnode manages the iOS devices flowing within a BYOD ecosystem with the help of secure Business Containers. These containers prevent attachments or documents from a managed source being opened in an unmanaged destination and vice versa. Furthermore, they avoid sharing documents from managed apps using AirDrop.

App management

The remote app life cycle management from Hexnode provides better support for BYOD. The seamless integration of Hexnode with Apple's Volume Purchase Program (VPP), Apple App Store, Google Play Store, and Microsoft Store simplifies the distribution of bulk purchased applications to the target devices. Additionally, the app management from Hexnode enables remote installation and uninstallation of specific apps, remote enforcement of app updates, mandatory installation of apps on devices, and much more.

Conclusion

Today, organizations are increasingly adopting Bring Your Own Device (BYOD) solutions to withstand the current competitive business world. The implementation of a BYOD scenario within enterprises can keep employees motivated to achieve the strategic objectives of their company. Furthermore, the BYOD program offers the potential to reconcile personal interests with organizational goals. However, leaving the employee-owned devices streaming inside a corporate network unmanaged isn’t a good idea. With greater access to enterprise data and applications, these devices can create more exposure to serious security challenges.



"According to the 2018 BYOD Security Report published by Bitglass, the Next-Gen Cloud Access Security Broker (CASB) solution, 85 percent of organizations are embracing BYOD based on a survey conducted by incorporating nearly 400 enterprise IT experts."

Source : Bitglass

A UEM suite can flawlessly address the security risks, threats, and vulnerabilities that can occur as a result of BYOD deployments within enterprises. The BYOD management solution from Hexnode provides excellent visibility and control over employee-owned devices, thereby encouraging the workforce to be more productive at work. The ability of Hexnode to enforce various restrictions and configurations to the target devices helps IT admins maintain regulatory compliance with corporate policies. Moreover, Hexnode ensures that the BYOD scenario can be managed perfectly without causing any hindrance to employee privacy. Therefore, BYOD security being a serious concern for IT administrators, implementing a UEM solution in the workplace is the most sensible approach to consider before beginning the voyage towards BYOD deployment.