White Paper

ManageEngine
Endpoint Central

Leveraging BYOD

ManageEngine
Powering IT ahead

Introduction

With the coming together of PCs and mobile devices, we are witnessing an unprecedented increase in enterprise mobility. Today, mobiles and tablets are ubiquitous in any work place. Employees access most of their business applications by using mobile devices. Some industries, such as education, manufacturing, and healthcare, have responded quite well to this trend, and they allow their employees to access corporate data by using mobile devices securely.

The Rise of BYOD

To understand the rise of BYOD, we'll need to consider the following trends:

- Rise of IT consumerization
- Enterprise ability in managing mobile technology

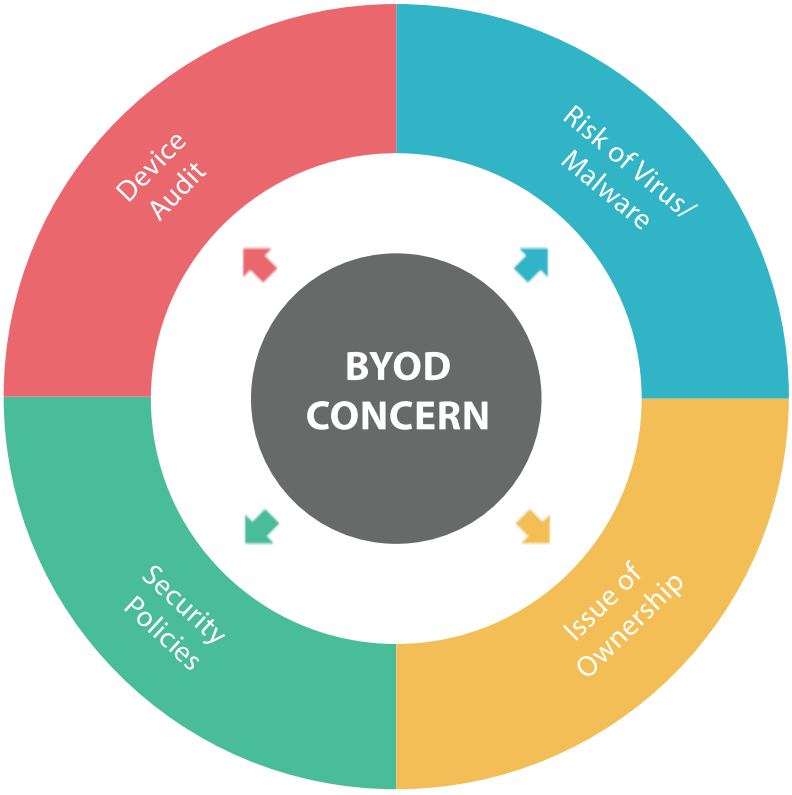
The awareness of technology among employees has risen with the rise in mobile device usage. Therefore, it's time for the IT teams to evaluate and understand the potential of BYOD.

Concerns

With the increase in BYOD, the concerns around it are mounting because of the threats to data integrity and data availability.

Meanwhile, many BYOD implementations are already experiencing significant prob-lems, including:

Device Audit: One of the primary concerns is device recognition. The IT team needs to constantly detect devices that enter and exit the company premises. IT administrator could use network access control to define the security layer in the enterprise network to accommodate devices based on APIs. This can help in monitoring the users and the



users and the devices they access inside the organization. However, this solution is not foolproof because device can be isolated from the network without the ability to go through NAC checks. For example, in manufacturing companies, part time workers may access information from their own device with the edge network, which can make the data vulnerable to security attacks.

Risk of Virus/Malware: Using commercial apps and public hot spots to access emails puts your corporate data vulnerable to virus attacks. Hot spots are present in various locations, such as coffee bars, hospitals, movie theatres, etc., which might be vulnerable to security threats. Therefore, it becomes imperative for the IT team to establish stringent security policies.

Adherence to Security Policies: Enterprises will need to monitor carefully the devices that employees' carry because of the company data stored on the mobile devices. If the IT department does not enforce security policies, the employees may willfully disregard those policies and inadvertently cause security incidents.

Therefore, enterprises need to implement and ensure adherence to security policies without unduly restricting users' control over their own devices.

Issue of Ownership: In the case of BYOD, there's a constant tug of war between data and devices. Devices are employee-owned whereas data is company-owned. The rights associated with hybrid ownership can complicate BYOD tasks such as restricting access to official emails or performing a data wipe. In the absence of thorough usage and ownership guidelines, the advantages of BYOD might be completely lost.

Getting 100% from BYOD:

The adage, one size does not fit all applies to BYOD. Each industry has its unique set of requirements for managing employee-owned mobile devices. A perfectly tailored BYOD policy can give the best returns for an organization. To ensure that companies derive the maximum benefit from the BYOD concept, you need to implement a robust security policy.

User Acceptance: The IT team needs to implement an effective mobile strategy. Because organizations allow employees to use their own devices, employees need to agree to the conditions and terms of use imposed by the IT team. The BYOD policy must list the rights and responsibilities of the employer and the employee, including who is responsible for data costs.

To lay out an effective policy, the IT staff and legal team understands the pros and cons of BYOD and work coherently to put the policy suitable to the organization context.

Systematic IT Approval: The IT team will need to create an approval mechanism to allow or prohibit the employee from accessing corporate data. The IT admin must ensure that they receive 24 x 7 alerts on employees accessing the data. An advantage of this approach is the ease with which data can be erased in exceptional cases such as a theft.

Stringent Policy Configuration: You will need to apply strict passcode polices and restrictions to device features and Mobile functionalities such as sharing options, camera settings, multimedia options, and more. Depending on the industry, configurations need to be tailored so that data can be protected from outside threats. Few of the polices are data access limitation in accessing documents and mails, support for device types, approval process for establishing access to office resources, permission to access resources depending on the employees roles and responsibilities, inactive device management, etc. These are the few polices that lets IT team to minimize the data leakage.

Data Security: To build a security foundation, the IT team has to combine BYOD with robust mobile device management (MDM) features that can help protect data from outside threats. MDM features such as password policy, data wipe, and profile configuration can help in maintaining strong data security with maximum protection. Containerization is another solution that helps in segregating enterprise data from personal data.

To ensure that only trusted devices enter the network, you can integrate network access control and MDM software. The anti-virus license should permit installation on employee-owned devices.

Group Restrictions: Creating profiles that might enable certain privileges for a specific section of users can help in defining access like whom to what. To monitor data easily, you can perform segmentation at two levels:

- Organizational unit levels such as HR, R&D, finance, and marketing
- Employee level such as contract workers, fulltime, and temporary employees

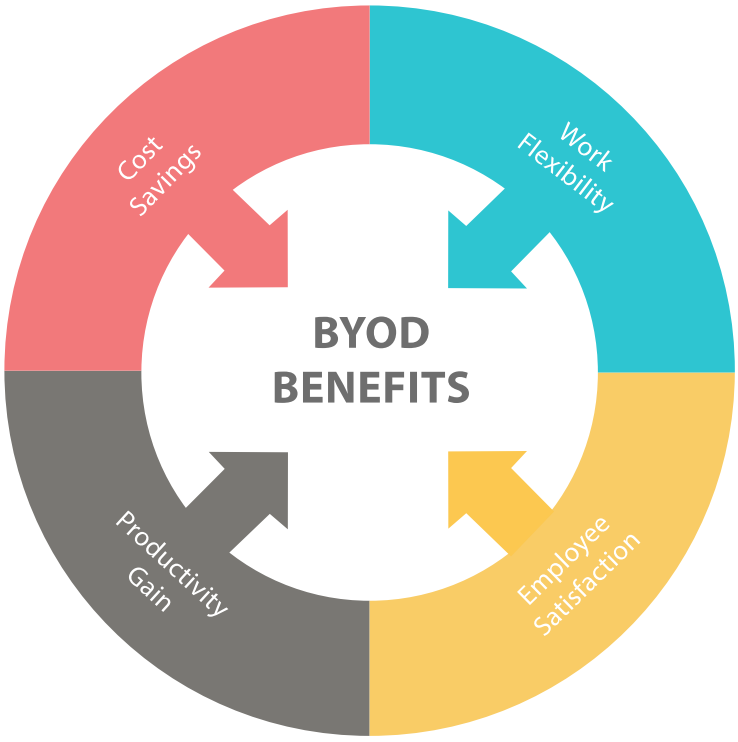
For instance, in the health care industry, surgeons might want to look at the patient's history before they begin any treatment, and the general physician might want to scan the patient's health status. In these cases, devices cannot be grouped in the same category. Here, it becomes essential for the IT admin to segregate devices based on the privileges and allow employees to use devices based on their roles and needs.

Harnessing BYOD: The IT staff cannot stop at implementing security policies. They must also educate employees on the importance of BYOD and its advantages. It is important to establish a mutual understanding between the end user and the IT team. The IT team must create guidelines and educate employees about the BYOD lifecycle, from self-enrollment to device retirement.

Device Retirement: Organizations need to implement an effective data clearance process to be followed when employees retire from the company's services. This will ensure that there is no data leakage and the company data is secure.

The best balance between failure and success: BYOD

Organizations need to evaluate the pros and cons of mobile technology trends and leverage them to fit their business framework. This section will briefly cover the driving forces of BYOD and its benefits.



Higher/Increased Productivity: BYOD helps organizations fully tap their employees' productivity. With technology that enables anywhere, anytime access to applications and data technology, conventional 9 to 5 jobs have been replaced with 24 x 7 availability. For instance, business development units are constantly on the move to meet clients in places like hotels and golf courses to discuss business, and it is of paramount importance for the sales teams to access their presentations on their mobile devices to complete their business successfully.

Cost Saving: BYOD reduces investment costs for enterprises by allowing work to be managed from an employee-owned device. The cost of the voice data is borne by the employees themselves or is supported by a reimbursement plan by the employer. Enterprises must implement and enforce a well-defined policy to keep such costs under control. This for instance can be done by providing VPN connection at the app level.

Work Flexibility: BYOD allows for work flexibility. Employees can access work-related information and complete tasks anytime, anywhere. With such flexibility, employees have a better sense of balance between work and life.

Employee Satisfaction: BYOD helps create a sophisticated work culture and an opportunity to reinforce a mutually beneficial relationship between employer and employee.

Best Practices:

- *Pre-determine the device types and operating systems to be allowed based on the available expertise.*
- *Scrutinize data that the device can access. Create a protocol to protect the data; the app should authenticate the user, encrypt the data, and disallow backups.*
- *Enforce stringent security practices, such as passcode policy, anti-virus applications, etc.*
- *Create data protection policies such as disallowing apps that read data from the device or app that transmits data to cloud, etc.*
- *Erase data from lost devices or retire the device and erase the data when the employee leaves the company.*

What lies ahead?

Despite the challenges that BYOD presents, it holds the key to the future because more and more employees rely on their smartphones and tablets for their personal and official work.

BYOD issues like employee privacy and hybrid and device/data ownership continue to challenge IT team. However, IT can still get the best out of BYOD by framing and implementing robust security policies. In these turbulent times, BYOD comes as a silver lining for enterprises to generate consistent productivity and run a profitable business.

About Endpoint Central:

Endpoint Central is a web-based server, desktop, and mobile device management soft-ware that helps in managing thousands of servers, desktops, and mobile devices from a central location. It automates the complete desktop management and mobile device management life cycle, ranging from a simple system configuration to complex soft-ware deployment.

Desktop offers a portfolio of features in Mobile Device Management like Profile Co n-figuration, Security Management, App management, Configurable reports, etc. With **Endpoint** Central, an IT administrator can manage iOS and Android-based mobile devices from enrollment to data wipe. For more details, Visit: http://bit.ly/17Pu4Te

About ManageEngine

ManageEngine serves more than 70,000 established and emerging enterprises - cus-tomers with IT infrastructures that are far more dynamic, flexible, and elastic than ever before. The net result is what ManageEngine calls real-time IT. Real-time IT calls for IT to make the most of today's game-changing technologies and deliver immediate services to organizations that are operating at an ever-increasing pace. It compels IT to operate at the speed of business, leveraging technologies to support new business models and applications.