White paper

BYOD

- A blessing or curse in disguise?

csg

Tomorrow's Technology Today

www.csgrp.co.uk

Contents

“Of the 15 million iPads on the street, half among them make their way to work; indicating a (BYOD) culture, that has already set its firm roots of growth”

Something evolving! What is it?

Talking about businesses today, things seem changed. Before our businesses could even wake to the reality of escalated usage of mobile phones, smartphones and tablets have come along to grab their own share in everything we do, right from the way we communicate to the way we work. Their portability and ease of use gives us access to any bit of information we may need regardless of where we are.

With every feature customizable, we can organize everything – right from our contacts, photos, videos, music, calendars, e-mail, information and also applications, exactly the way we want it and at its best for each one of us. And these are the very reasons why they have so profoundly found a place in our lives, and especially at our organisations.

BYOD - A brief

BYOD (Bring Your Own Device) is a term, which represents the culture in which the employees bring their personal computing devices like smartphones, laptops and PDAs, to their workplaces and use it within the corporate networks, to accomplish their corporate tasks.

For certain businesses, BYOD is an approach where an organisation provides flexibility to its employees to use their personal devices in corporate network, along with devices offered by the organisation. In a BYOD culture, an employee is permitted to use his/her own personal device to access enterprise end user computing resources like email, intranet, business applications etc.

Well-nested, already!

BYOD is no process or procedure; it is a trend which is growing rapidly. Of the 5 billion mobile phones, users across globe possess; 1.08 billion are smartphones. This clearly proves the extent to which smartphones have penetrated in terms of usage. Among all the smartphone users, 89% of them use it throughout the day, indicating the influence these smartphones have on all activities a smartphone user does in a day, which also includes his work. With more and more people purchasing and using these smartphones, assumptions of these phones entering organisations can be believed. With the highest smartphone penetration rate of 62% being in the 25-32 age group, it’s a believable fact that smartphones make their way to work.

Talking about tablets, in terms of stats, 11% of adults already own a tablet computer of some sort, of which 77%, use their tablets everyday [Source: Pew Research Center & The Economist Group]. Elaborating on terms of usage, tablet owners spend an average of 90 minutes on them per day and around 56% of tablet users say they use it several times a day [Source: Report by InMobi & Mobext]. User friendliness and its attribute of being mobile, makes it a must have device for some. The penetration level of tablets ensures their presence in organisations.

This sudden smart-phones and tablet popularity has taken many enterprises by surprise. The effects of increased usage of tablets and smartphones can be clearly seen on organizations and the way they are functioning today. Of the 15 million iPads on the street, Forrester Research figures say that half among them make their way to work; indicating a culture that has already set its firm roots of growth.

“Employees today have attached their personal devices to their workflows. Whether somebody chooses an Apple or an Android or a Blackberry or a Windows device, it is now about including these devices to a network.”

An ‘Enterprise Revolution’ in Making

With the increasing sales of these devices, BYOD is now more than what it was actually perceived. It has a more positive and acceptable reputation in enterprises today, as enterprises are constantly expanding and the roles of employees are ever evolving. Teams now include people that may be around the road virtually or at their desks. People come from all around the world, doing various tasks and hence the nature of their jobs involves a range of devices, to address consumers.

Hence employees today have attached their personal devices to their work flows. Whether somebody chooses an Apple or an Android or a Blackberry or a Windows device, it is now about including these devices to a network.

CIO, CTO and IT heads are now looking for a highly collaborative workspace or rather are expecting a work culture in which anyone can join in from anywhere using anything. The idea of people being hooked to their desks is no longer acceptable as mobile experience has indeed transformed the way organisations do their business today. Hence more and more enterprises and businesses are embracing the BYOD culture rapidly.

Teams today use their personal devices when they need to connect with clients, or they need to connect internally. And with BYOD culture they can do this quickly, efficiently and in a much more productive manner. IT teams today aim to build an ecosystem around unified communications, as BYOD demands for one.

Keeping in mind these statistics and trends; predictions of more enterprise embracing BYOD seem more real. Apart from these, enterprises also have convincing reasons to allow employees to use personal devices for work – including Productivity enablement, Business IT capital cost savings, Social collaboration enablement, workplace trends elsewhere and ‘because the employees want it’ phenomena.

Despite the potential security risks and concerns, permissions to use these devices are growing tremendously among several enterprises. IT administrators have started designing new policies that support usage of these devices to access network resources, in an attempt to balance security and productivity together, using BYOD.

“(BTOD) brings a whole new set of concerns for IT administrators… Organisations are now worried about securely introducing these devices into the enterprise networks.”

Security Care – takers see it Red!

BYOD has already arrived, well before we thought it would and as it comes it brings a whole new set of concerns for IT administrators. Organizations are now worried about securely introducing these devices into the enterprise networks. The main question is, ‘Can these devices be controlled using the same security policies, like company-issued devices?’ Well, answer to this is both a Yes and a No.

Talking about security solutions, organizations should opt for a solution that offers both, threat prevention and data protection. There are numerous security providers for dynamic and mobile scenarios, but only a right and apt solution will work. The right solution should offer the ability to minimize incidents of data loss or leakage, collectively.

Visibility

At every organisation, in order to ensure security, productivity and connectivity, IT department needs to know who is on the network, where the user is, what type of device the user is using and what the status of the device is. Visibility to granular levels can ensure smooth functioning among teams of an organisation. Under the BYOD scenario, it becomes very difficult to monitor all these various devices that keep coming in and leaving the network anytime.

Network Security

Under a BYOD culture, unlisted personal devices owned by varied people, joining in to the company network, increase the chances of infected devices transmitting viruses to the network, thereby also infecting the other devices connected to the network.

Data Leakage

With the arrival of new devices to network, ensuring network security becomes a top priority. With 63% users sharing their tablet with 2 or more people [Source: UM Research], securing data on such devices is a challenge. This becomes a major concern for organizations that deal with confidential data, as users may use their personal device to download/access organisational data and once out of the network may hand over the device to someone who is not so loyal to that data. Talking about data leakages, there exist 2 scenarios that can lead to data leakage in a BYOD scenario and they are Unsecure Network Access and Device Loss or theft.

Unsecure Network Access

With the BYOD scenario making Internet use convenient, owner of these devices may access unsecure sites or make use of random unauthorised apps that are not properly configured for security, opening the doors for sensitive corporate information stored on that device to go out.

Device theft

Too many devices accessing the corporate network increase the threat of data loss through device theft or device lost. Device theft comes with the anticipation that malicious users can access sensitive information stored in it. The danger grows severe when the data accessed, using the lost device, was sensitive information.

"In a BYOD scenario, administrator should have the right to dictate, which user or user device can access network resources, what amount of network resources can the user access based on parameters like time for access, bandwidth availability, applications used, websites accessed, and more, along with the visibility of, which user or user device used what network resources."

Bandwidth crunch

Apart from security, the strain personal devices, viz. iPads will put on wireless networks, has everyone concerned. The network administrators are already crying out loud about their concerns on network security and the alarming network usage that are becoming a reality with the new BYOD culture. Keeping the iPad protected and updated with new functionalities is a continuous job, and also a huge drain on an organization's network resources as updates and upgrades can be several GBs in size. With multiple iPad users in an organization, impact of this on the network is tremendous. Reducing the effect of such bandwidth crunch on business networks has become crucial and urgent.

Should every organisation, adapt this new hype?

Having said that the prime question to be asked is, 'Does your organisation need to adapt BYOD?' While considering the decision to adapt BYOD, organisations should start with evaluating the consequences, if their employees were to use personally owned devices, for organisational work. Quantum of benefits and risks should be estimated, accordingly, before venturing into this new dynamic culture of BYOD. For organisations like the ones offering defence services or those dealing with highly sensitive data, BYOD may not be the right choice, especially considering the consequences on data leakage. Whereas, for SMEs with cost cutting on their main agenda, BYOD may be a blessing, with reduced costs on inventories, as devices used in BYOD culture, are owned and maintained by employees at their own expense.

Like every other innovative culture, BYOD for sure, comes along with numerous productivity and connectivity benefits, but security still remains a concern. Before deciding on imbibing BYOD at your organisation, it's good to evaluate what are your priority essentials. It is good to know, whether your requirement is productivity or security.

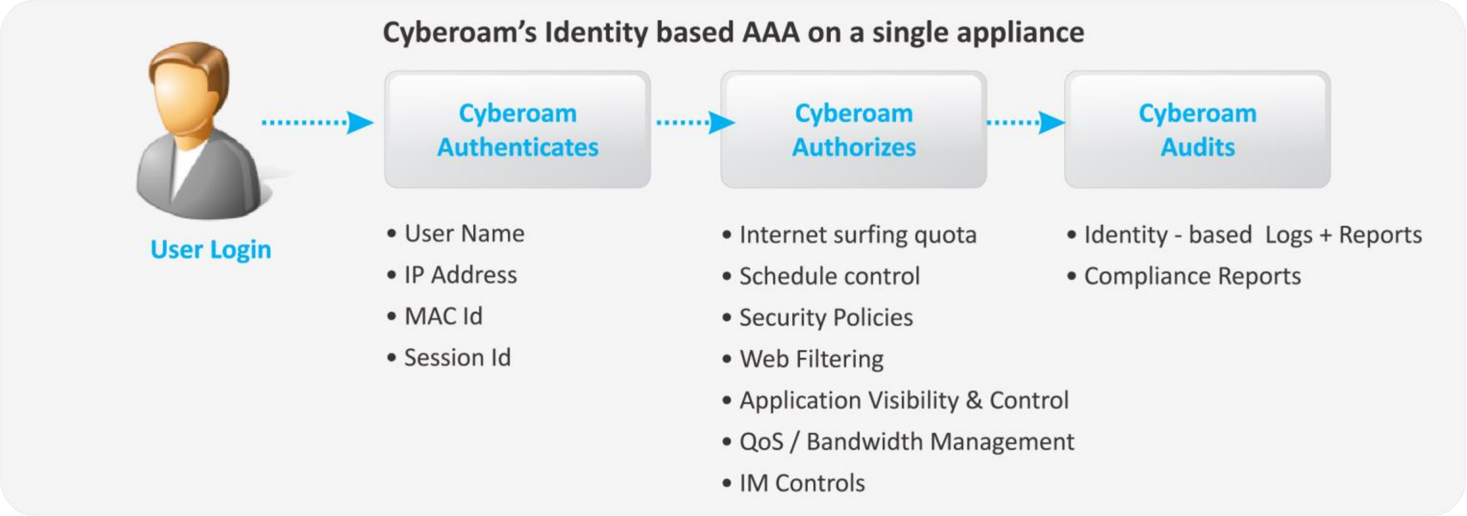
Just for a matter of understanding, let's take the example of air travel. Air travel was considered as the riskiest mode of travel, as most air accidents did not leave any survivors. But the point to be noticed is, whether these facts and risks, anyway hinder in air travel being used as a mode of travel. The answer is no. As we all know, avoiding air travels was never a feasible idea; hence considering its high utility and necessity, steps to ensure security were taken. Today, air travel is the safest mode of travel in the world, and the air travel industry has achieved this, by understanding the risks and implementing measures to ensure security.

A Safety Wrapper around BYOD

Talking about control, IT departments have little or limited control, over unlisted personal employee devices. Hence the best policy for security is to have visibility and control over what devices are getting connected to the network and by which user, along with having the flexibility of extending the security and network access policies that exist for a user, to all the new devices the user brings into the network. In a BYOD scenario, administrator should have the right to dictate, which user can access network resources, what amount of network resources can the user access based on parameters like time for access, bandwidth availability, applications used, websites accessed, and more, along with the visibility of, which user or user device used what network resources.

Why Cyberoam?

Cyberoam UTM's unique Layer 8 Technology allows network administrators to design identity-based policies, which extends throughout the network, irrespective of the device used by the employee to connect to the network. Cyberoam UTM offers secure identity-based AAA (Authentication, Authorization, Audit) over a single device, allowing control and knowledge of who is connected to your network, using what device and what they are accessing. You can design security policies that allow you to decide, what each user/user group can access in terms of websites/applications over Internet and for how long, the amount of data transferred and bandwidth they can consume.



Cyberoam's Identity based AAA on a single appliance

User Login

Cyberoam Authenticates

- User Name
- IP Address
- MAC Id
- Session Id

Cyberoam Authorizes

- Internet surfing quota
- Schedule control
- Security Policies
- Web Filtering
- Application Visibility & Control
- QoS / Bandwidth Management
- IM Controls

Cyberoam Audits

- Identity - based Logs + Reports
- Compliance Reports

Conclusion

With increasing numbers of smartphone and tablet sales, these devices will no doubt become more prevalent in the business world. Both employers and employees are voicing their views about the gadgets they want to use for work, and IT is confronted with issues to identify BYOD strategies, in order to fulfil the requirements of these gadgets.

BYOD no doubt is very flexible and highly useful, but it presents some grave challenges to organizations like, ensuring that unauthorized devices are prohibited from using organizational infrastructure, to assure network security and rightful usage of network bandwidth.

CSG COMPUTER SERVICES GROUP

- **BRIDGEND**
- **BRISTOL**
- **EXETER**

T: 0845 051 5508

E: SALES@CSGRP.CO.UK

csg

Tomorrow's Technology Today

www.csgrp.co.uk