SECURING ENTERPRISE NETWORK – 3 LAYER APPROACH FOR BYOD

1. Wireless Network Infrastructure
   - User Experience
   - Device Security
   - High Performance

2. Mobile Device Management
   - Configuration Management
   - Policy management
   - Security Management

3. Network Access Control (NAC)
   - Identity Management
   - End point Security
   - Usage policy Enforcement
# Table of Contents

- Executive Summary ........................................................................... 03
- Introduction ....................................................................................... 03
- Challenges ......................................................................................... 04
- Solution .............................................................................................. 05
- Three Layered Approach to secure BYOD ............................................. 06
- Conclusion .......................................................................................... 07

# Table of Figures

- Figure 1 Integrated Wireless, MDM and Access Management .................. 05
- Figure 2 Three Layered Approach to secure BYOD ................................. 06
Executive Summary

Enterprises derive significant benefits by implementing a Bring Your Own Device policy. These benefits include increased productivity, reduced costs, better business continuity and enhanced employee satisfaction. However, BYOD has its set of challenges and security vulnerabilities that come along when random and multiple devices with varied operating systems and dissimilar features are introduced into a secure network. Companies have the onerous task of managing the increased complexity of their networks and simultaneously delivering a secure, high quality user experience. There is the need for a unified and secure architecture across wired and wireless networks to provide the BYOD benefits without compromising on network security.

Introduction

Gartner predicts that by 2016, at least half of enterprise email users will rely primarily on a browser, tablet or mobile client instead of a desktop, reflecting the increasing amount of time that employees are spending at remote locations. The secured usability of handheld and tablet devices in a corporate work environment has therefore become a necessity at many enterprises.

For a cost concerned organization, buying or replacing so many end devices would create budget challenges. However, as most employees already own such devices, it makes sense to use one compact unified computing and communication device for personal and official requirement. According to Cisco Systems’ annual Visual Networking Index Forecast released in June, by 2015, there will be almost 15 billion network-connected devices—including smart phones, notebooks, tablets and other smart machines—more than two for every person on the planet.

To tap into this device growth, enterprises are actively evaluating and adopting Bring Your Own Device (BYOD), a concept where employee owned mobile devices are securely allowed inside a corporate network for accessing one or many of intranet applications.

While a BYOD may seem like an easy solution to execute, there are numerous underlying access and security threats that an IT group has to consider before implementing such a solution. According to the recent Ponemon study, 51% of the organizations surveyed in its study experienced data loss in the last 12 months that was a result of employee use of insecure mobile devices; this includes laptops, smart phones, USB devices, and tablets. This white paper outlines the key challenges and the solutions that an organization can implement to benefit from BYOD without compromising on network security.
The three security challenges mentioned below have to be comprehensively addressed for a successful BYOD adoption.

**Availability of Secure and Seamless Wireless Access**

Tablet and handheld devices use wireless as the medium for communication with external devices. Therefore, the end user experience of BYOD depends on the seamless availability of wireless coverage and capacity planning. Some of the wireless technologies that have gradually gained acceptance on mobile devices are 3G, Wi-Fi and Bluetooth. As 3G services are restricted to service providers, and Bluetooth is not suited for network communications, Wi-Fi has become the most preferred wireless LAN technology in an enterprise environment.

Wi-Fi is an open standard protocol and operates on unlicensed frequencies, which increases the network vulnerability to rogues and other security threats. Organizations need to secure the RF environment before a wide scale adoption of BYOD.

With the proliferation of services, enterprises have begun to understand the importance of the right SOA Governance Framework. They have introduced specific roles to govern the service lifecycle and streamline services using the right governance processes. Many enterprises have therefore adopted industry canonical models to incorporate best practices and consistency in service analysis and design. Today, the usage of industry models for defining services is predominantly focused around interface and message models neglecting business process models. This is mostly because enterprises use several business process versions that lack proper documentation and are reluctant to change/standardize existing business processes.

**Management of end devices and enforcement of corporate policies**

Most of the laptops and desktops used today by enterprises run in one or the other version of Microsoft Windows Services. In such a scenario, managing end devices and enforcing corporate policies, audit and remediation of non compliance is far easier to achieve. When a user brings in his/her personal device, it is unsecured as none of the access policies have been enforced on it.

Some of the security vulnerabilities from such devices can be in the form of viruses or spywares apart from the physical security breaches such as cameras and USB interfaces. Hence installing a new device into the network has to be undertaken with utmost caution in a BYOD environment. Multiple devices with varied operating systems and dissimilar features add to the complexity in policy enforcement, physical theft, malware prevention, IT support and employee education.

**Control on the network devices and end points**

The third challenge that an IT manager faces when deciding on BYOD is the control required for the network devices and end points. Profiling and posturing mobile devices must be completed before a network can allow access for a user. Allowing guest users into the network, again poses challenges to organizations especially when the nature of the guest’s device is unknown. Segregating and securing guest traffic without complex changes and additions of VLANs is an increasingly vital challenge that an IT manager has to contend with.
The wireless infrastructure should support 802.1x authentication using EAP to provide a framework with protocols that allows user authentication by a central authority. A robust wireless network infrastructure allows for securely connecting devices, optimizes the voice and video experience, and protects overall performance by avoiding interference. Cisco and Aruba are the market leaders in providing wireless infrastructure which comprises of a Wireless LAN controller, access point, location tracking, intrusion prevention system and a management system.

A Mobile Device Management (MDM) solution is an application suite that allows entry of BYOD devices in a corporate network by simple management and authorization based on device profile and fingerprinting. Afaria, Mobile Iron and Zenprise are some of the MDM solutions that can support multiple operating systems and device management functionalities.

A true MDM solution should support policy management, security management and configuration management. Configuration management includes device provisioning and policy pushing based on the contexts like device type, user group, time and date. Security management would offer encryption, certificates and token based authentication and data protection features like remote backup and wipe out of data and authentication credentials. Application management and device health management modules are the other important modules in an MDM.
**Network Access Management Solution**

A comprehensive network access management solution is imperative in a situation where corporate network access policies have to be pushed both on the wired and wireless users. A survey published by the Boston Research Group today suggests that 78% of IT security professionals believe that Network Access Control (NAC) is an essential component and must be a major part of any BYOD security solution.

A network identity and access management solution complements MDM by providing additional security. A device is finger printed, profiled and postured before it is allowed for any kind of access in the network. Avenda System’s clear pass and Cisco Integrated Security Engine (ISE) offer a comprehensive and centrally managed policy engine which allows network access policies to be pushed on to the end devices like laptops, desktops and tablets and the network devices like switches and wireless LAN controllers.

The network is fully context aware and access rights can be granted to users based on different parameters like time, location, device type and authorization level of a particular user. Auto provisioning algorithms built in this solution considerably reduces the pain of provisioning multiple devices at multiple locations. The auto Guest provisioning is another important feature which increases the overall user experience when guests need to use their devices.

**Three Layered Approach to secure BYOD**

The three-layered and unified approach is required to achieve network access control and operational efficiency.

---

*Figure 2 Three Layered Approach to secure BYOD*
802.1x and EAP complete the authentication of network credentials before a network IP address has been assigned, thus preventing and mitigating threats before they can spread into the enterprise network. However, when an end point device physically or logically moves to other wireless networks, additional network profiles are added to the device configuration. This sprawl of network profiles on each device locally affects the user experience as well as poses a security challenge to IT organizations.

MDM allows efficient use and cost effective management of a large number of devices and is therefore a critical enabler for BYOD. MDM systems typically control access to applications but not to the network. They are blind to unmanaged devices on the network. Therefore, MDM does not prevent unauthorized access to data on the network, nor does it prevent infected or compromised devices from attacking the network.

NAC enhances network control, security and visibility. NAC augments 802.1x to provide dynamic profiling of end point devices, endpoint compliance validation and advanced management of guest access. NAC can use 802.1x as a base for identity authentication and then include other posture credentials to extend the authentication process. The integration between 802.1x and NAC enables the identity and posture credential check to occur in a single 802.1x transaction.

**Conclusion**

For BYOD network security, a unified approach comprising three key complementary solutions robust wireless infrastructure, Mobile Device Management and Network Access Management, should be taken. The wireless network enables mobility; MDM helps manage large scale deployments and Network Access Management mitigates the threat that devices pose to the network.

Employees demand for a unified device for all communication and computing is driving the adoption of BYOD in a corporate environment. The ease of user enrollment and mobility advantage are other compelling reasons for enterprises to adopt this emerging phenomenon.
About Wipro Infotech

Wipro Infotech, the India, Middle East and Africa business of Wipro Limited (NYSE: WIT) is a leading Information Technology, Consulting and Outsourcing company, that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of “Business through Technology” – helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner’s approach to delivering innovation and an organization wide commitment to sustainability. Wipro’s IT business has over 130,000 employees and clients across 54 countries.

About the Business Unit

Systems Integration is a part of the Professional Service Division in Wipro. The Business unit has several consultants who provide thought leadership across solutions for various domains. The services offered include the following:

1. Advisory Services
2. Network Design
3. Network Build and Transformation

About the Author

R Senthil Kumar

Senthil Kumar is the Technical Consultant for Wireless Mobility Solutions in System Integration business unit. He has over 11 years of experience in the industry. He has handled roles in Solution Architecting and Solution Delivery. He has extensive experience in Consulting and Design and Implementation of multiple wireless technologies for various business transformations.

Manishankar Rajagopalan

Manishankar works as a Practice Head in the Systems Integration Business Unit and has over 17 years of industry experience in the wireless and wireline domains. He has handled various roles in Business Development, Consulting and Solutions.