BYOD Solution Overview

Revised: August 7, 2013

Introduction

Bring Your Own Device (BYOD) continues to be one of the most influential trends reshaping the landscape of the mobile enterprise and the evolution of IT organizations. The influx of powerful mobile devices into the workplace is changing how users access and consume enterprise resources. IT managers are establishing policies with BYOD access as the norm rather than the exception due to increasing demands from employees and executives who embrace this megatrend. Enterprises are beginning to see BYOD as an opportunity rather than a challenge. There is no longer any doubt that enterprise IT departments are adapting to mobile devices (smartphones, tablets, laptops, etc.) in the corporate workplace to meet user expectations and leverage new technologies to boost worker productivity.

IT needs to balance productivity with security and coordinate business justification with the various line of business (LOB) owners to implement BYOD programs within an enterprise. On one hand, employees are demanding access from devices not only within the corporation, but also beyond the firewall. On the other hand, risk management dictates that corporate data must remain protected

The Cisco BYOD Smart Solution delivers a unified workspace that increases workforce productivity with high quality collaboration on any device, anywhere. Cisco BYOD Smart Solution is a complete, yet flexible and secure BYOD solution that one can easily tailor to meet an enterprise's needs. Cisco customers get proven solution designs that are fully system tested and documented in a Cisco Validated Design (CVD). The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments.

When BYOD is properly implemented, it delivers an uncompromising, work-your-way user experience and enables organizations to secure data with unified policies and essential controls.

BYOD Market Landscape

Mobile devices are turning into general computing devices with faster components and better integration and support in connecting to enterprise systems. They are being used by employees to perform their regular job functions. In many cases, each employee owns multiple devices which they use for personal as well as business work.

The BYOD market was initially centered on allowing employees, partners, and guests to connect to the corporate networks and be able to perform a limited number of basic functions, such as access the Internet, access corporate email, calendar, and contacts, etc. As more and more personal devices become

prevalent in the enterprise, workers are using these devices to access enterprise resources and applications to do their daily jobs. With employees using personal devices for mission critical job functions, mobile device managers (MDM) are becoming increasingly important. Functions such as ensuring that a device can be locked and wiped remotely in case it gets lost or stolen or when the employee is terminated are becoming a necessity.

An enterprise's BYOD strategy should build momentum towards meaningful infrastructure, security, and wireless innovation and provide a solid rationale for BYOD investments.

To understand the benefits and the challenges BYOD poses, it is helpful to understand the business trends that are hindering or driving BYOD adoption.

BYOD and the Enterprise Network

The network is at the heart of all business functions and is a key enabler for service delivery. With the proliferation of mobile devices, protecting enterprise networks is getting more complex. Inconsistent management tools and policies across the wired and wireless segments of the network can increase the burden for network managers and drive up management costs and complexity. An architectural approach and design can help businesses realize greater levels of manageability, enhance user/customer experience, provide greater levels of flexibility and performance, and achieve improvements in security and policy.

Today enterprises have diverse wired and wireless LAN infrastructure implementations. The traditional workforce model involves a worker going to an office and performing their job functions while tethered to an IT-provided computer and an IP phone. Hence the focus has been on ensuring that the wired enterprise infrastructure is robust and secure. The wired network is built for high availability and performance, with adequate capacity and intelligent features such as QoS to make phone calls, exchange data and video, etc., within and outside of the enterprise. Communication within the premises is based on a trust model, protected by firewalls at the perimeter and other security tools.

In contrast, the enterprise wireless infrastructure was built for convenience, at least until the BYOD phenomenon emerged. With BYOD, users will have three or more mobile/WLAN devices (laptop, tablet, Smartphone) all connecting to this infrastructure. The devices themselves could be user-owned or corporate-owned. What is the trust level of these devices that are accessing secure enterprise resources? How are they accounted for at all times? With all these questions demanding answers, one can expect a lot more focus on the wireless network. The WLAN needs to become as robust, secure, scalable, and predictable as the wired network to support BYOD.

BYOD Security and Policy-Many enterprise CIOs and architects cite security as a major inhibitor in the deployment, adoption, and acceleration of BYOD within their enterprise. It can be overwhelming to manage security for various applications for a huge set of new BYOD devices with diverse operating systems and users. Based on each customer's environment and business policy, there are many options for implementing and configuring personal and network firewalls, intrusion prevention, anti-spyware, data security, device control for smartphones, desktops, and tablets for various user roles such as employees, guests, partners, and remote workers.

Policy management is critical to a successful BYOD strategy which enables endpoint security for multiple devices and diverse user roles. Application management and security are on the rise in a BYOD environment as enterprises seek to manage and secure applications rather than devices, with more granular policies applied based on worker or application type. More companies want enterprise application stores that allow for a central deployment method. The security needs of a mobile workforce include:

- Ensuring that the devices used to access the corporate network are safe and are not jail-broken or rooted. They should not have threatening malware, spam, or applications that can compromise the corporate network or data.

- Making sure users and devices that are accessing the corporate network can be identified and allowed connectivity only if they are authorized and meet company policy.
- Securing access with client-based or clientless access to ensure data loss prevention with encryption or containerization with VPN optimized for efficient application delivery and capabilities.
- Enforcing device-level security functionality such as remote wipe/lock with integrated Network Access Control (NAC), thus ensuring that an action can be taken on non-compliant devices at any time (not just during access).
- Having visibility into users, devices, and the applications they are running on the corporate network.

Mobility—The hottest segment of the enterprise networking market is wireless LAN equipment to support enterprise requirements for user mobility and wireless devices. As smartphones and tablets become more powerful, they are increasingly used by employees to connect to the WLAN and other enterprise resources to do their normal job functions. It then becomes important for the WLAN to have same or similar intelligence and feature functionality, such as high availability, QoS, local switching, application visibility and control, ease of collaboration, etc., that users have become accustomed to on a wired infrastructure.

Role of MDM in the Enterprise Network

Mobile Device Managers are designed to help an enterprise rapidly and securely deploy mobile devices and applications with policy, compliance, configuration, and application management to minimize risk. Large enterprises are extremely interested in delivering general-purpose as well as custom-built corporate applications to their workforce (for example, mobile sales force automation applications).

BYOD security and device management are the foundations of an enterprise BYOD strategy which must consider all mobile worker types and functions before deploying solutions. Organizations need to consider solutions across the security sub-segments that secure endpoints, provide protection for the corporate network, and protect data as it moves over their infrastructure.

The ability to integrate MDM functionality, coupled with a policy-based network access, ensures that legitimate devices and users can access the network and attempted violations can be controlled by prohibiting or limiting access to the network or network resources.

User Need and Role of IT

BYOD connectivity may look like a simple extension of enterprise mobile services, however broad user expectations and the diversity of devices create unique infrastructure demands and challenges for IT operations with end-to-end and network optimization and lifecycle management to support BYOD.

Device choice does not mean sacrificing security. IT must establish the minimum security baseline that any device must meet to be used on the corporate network, including WiFi security, VPN access, and perhaps add-on software to protect against malware.

In addition, due to the wide range of devices, it is critical to be able to identify each device connecting to the network and authenticate both the device and the person using it.

Protecting Data and Loss Prevention

One of the largest challenges with any BYOD implementation is ensuring protection of corporate data. If a corporate asset, such as a laptop, is used to access business applications and data, typically that asset is tightly controlled by IT and likely subject to more restrictive usage policies.

Some industries need to comply with confidentiality regulations like HIPAA, security compliance regulations like PCI, or more general security practice regulations like Sarbanes-Oxley and others. Companies need to show compliance is possible with BYOD adoption, which can be more challenging than with a corporate-owned and managed device.

An employee-owned mobile device is likely being routinely used for personal access and business applications. Cloud-based file sharing and storage services are convenient for personal data, but can be potential sources of leakage for confidential corporate data.

IT must have a strategy for protecting business data on all devices whether corporate managed or employee self-supported and managed. This may include a secure business partition on the device which acts as a container of corporate data that can be tightly controlled and may also include the need for a Virtual Desktop Infrastructure (VDI) application to allow access to sensitive or confidential data without storing the data on the device.

At some point in the lifecycle of a device or employee, it may become necessary to terminate access to the device or the device's access to the network. This could be due to a lost or stolen device, an employee termination, or even an employee changing roles within the company. IT needs the ability to quickly revoke access granted to any device and possibly remotely wipe some or all of the data (and applications) on the device.

Challenges for End Users

BYOD solutions and technologies are quickly evolving, however one of the largest challenges is how to make it simple for people to get connected to and use corporate resources and applications to do their work. The number of device possibilities, the range of connection types and locations, and the lack of widely adopted approaches can translate to difficulties for users.

Security precautions and steps may also vary depending upon how and where the user is trying to connect. For example, the corporate WiFi may require credentials, whereas connecting through a public WiFi hotspot may require credentials, a virtual private network (VPN), and other security steps. If such security measures are too intrusive, they could erase productivity gains of BYOD.

Key Advantages of the Cisco BYOD Solution

- Cisco networks are integrated into one control panel, resulting in greater security and ease of management.
- The Cisco Solution relies on a centralized policy server that integrates tightly with an organization's Active Directory and PKI infrastructure.
- Fully integrated, centralized, single point of visibility and control of users, devices, location, network, and applications resulting in greater security and ease of management.
- Services across end-to-end partner ecosystem—Pre-integrated and tested solutions with world-class partners.

The Cisco BYOD solution integrates the Cisco products, third-party products, and devices discussed previously into a comprehensive BYOD approach which is tightly integrated across the network infrastructure. This offers a unique set of advantages such as flexibility to allow for multiple diverse user groups, including deskbound workers, mobile workers, customers, guests, etc.