Empower employees with device freedom without compromising IT Network

A Bring-Your-Own-Device (BYOD) Solution Brief

Introduction

Bring Your Own Device (BYOD) has become one of the most influential trends that has or will touch each and every organization. The term has come to define a megatrend occurring in IT that requires sweeping changes to the way devices are used in the workplace.

What is BYOD? It is about end users being able to use the compute and communication devices they choose to increase productivity and mobility. These can be devices purchased by the employer, purchased by the employee, or both. BYOD means any device, with any ownership, used anywhere.

This solution brief discusses how this trend will affect businesses, explores the challenges it creates for IT, and outlines the various components that are part of our solution.

Layer3 offers a comprehensive solution from Juniper Networks to address these challenges, allowing end users the freedom to bring their choice of device to work while still affording IT the controls to ensure security and prevent data loss.

The Challenge

BYOD is already a challenge for many organizations and it might feel like an invasion by UFOs. IT departments need to review if employees can access the company network with mobile devices in a secure, reliable way independent of the established technology. In the past, one has tried to secure end-user devices with things like Network Access Control (NAC), but with the fast increasing amount of different types of devices and platforms, the past attempts lack support for the end-users and don't offer easy access to applications.
The challenge lies in being able to support employees in their choice of working method without having to reduce or jeopardize security.

The influx of new devices create two main challenges for network administrators:

1. Providing easy and appropriate resource access
2. Creating a secure environment for mobile, non-corporate devices

Providing Easy and Appropriate Access

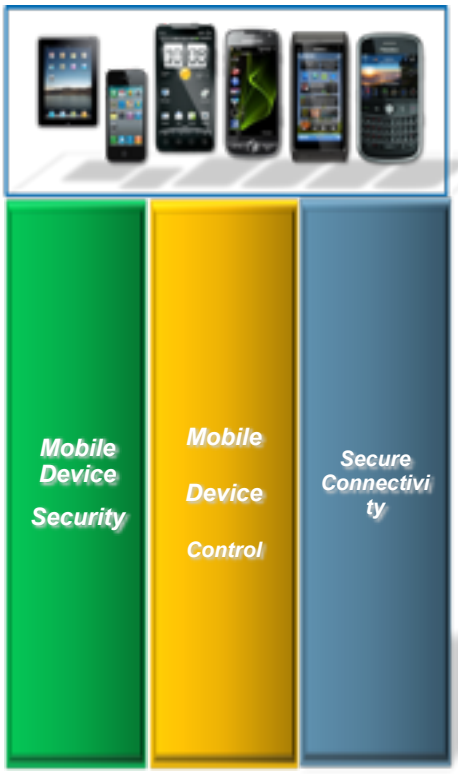
Users must have simple ways to register their devices on the network that does not breach security policies established by the workplace. Also, different classes of users from guest, to staff to temporary workers must receive different access privileges, but one that is easy to administer by resource limited IT departments. The process of "onboarding" a device – bringing a new device onto the network for the first time - should be simple and a self-service process without the need for IT intervention. Furthermore, onboarded devices ideally require little or no installation of software clients on their device to manage the transition to secure access of device on the network.

Creating Secure Environments

It is important to ensure that people and devices are authenticated prior to receiving network privileges. The enforcement of security policies are granted during the onboarding process of each new device. In addition, security parameters such as 802.1x, and encryption between the device and the Wi-Fi network are critical. IT administrators must have visibility to not only secure the device but often also applications that may or may not be allowed to run on those devices. Administrators must be able to:

- Enforce network policies
- Protection of Data loss and Device loss
- Revoke Access – removal of access from the network

Layer3's Solution



Layer3's BYOD solution helps you embrace BYOD while preserving security. The solution, which runs on Juniper Networks' Junos Pulse Access Control and Mobile Security Suite, gives you real-time visibility and control over personal devices on your network.

The Junos Pulse Mobile Security Suite, a component of the solution, protects and manages mobile devices, their users, and their apps. It delivers comprehensive mobile device security, management, monitoring and control. It protects smartphones, tablets and other mobile devices from viruses, malware, loss, theft, physical compromise, and other threats, as well as delivers secure mobile device management for enterprises and service providers. The solution offers services that are purpose-built for mobile devices, including:

1. **Antivirus**
2. **Anti-malware**
3. **Loss and theft prevention**
4. **Mobile device management, monitoring and control**
5. **Mobile endpoint firewall**
6. **Anti-spam**

KEY BENEFITS

- See 100 percent of the endpoints connected to a corporate network. Identify devices the moment they try to connect to your network.
- Grant, deny, or limit network access based on who and what is trying to access your network including mobile devices such as iPhone, iPad, Android, etc.
- Identify the sources of malicious attacks and quarantine the systems to protect your network. Control risky behavior and unauthorized applications on all systems.
- Save time by automatically detecting which endpoints do not have the required security agents and automating the installation of those agents.

Junos Pulse Access Control Service, another component of the solution, delivers identity-based, location-aware, granular access control with robust mobile and non-mobile endpoint device security and integrity checks. It delivers comprehensive Layer 2 admission control, Layer 3 access control, or both for the most dynamic, granular identity- and role-based network access control,

Layer3's BYOD solution delivers global identity-aware networking, complete with security and access control policies that follow a user around the globe, no matter from where, how, or from what device, including mobile devices, they use to access the network.

Know who is accessing your network and its resources, when, how, from where, and through what device. Only Layer3, using Juniper's Junos Pulse Access Control Solution, can deliver this level of worldwide secure access control.

The Layer3 Advantage

Layer3 has years of experience designing, deploying and supporting complex networks. Our partnership with some of the global leaders in networking and security solutions enables us to provide best-of-breed solutions to our customers. We offer varying SLA options to support your unique needs. By choosing Layer3, you can access our wide variety of services, world-class service delivery, consistency and peace of mind. We offer the following advantages:

End-to-End Infrastructure
Our privately managed MPLS network provides exceptional performance, total redundancy, and the flexibility to deliver true Quality of Service.

Complete Service Portfolio
We offer a full range of business data, network, security and hosted IT services.

Unbeatable Experience
We have been serving some of the most demanding businesses with innovative services for 7 years and have the highest industry technical certifications within the region.

Superior Customer Support
Our friendly technical experts respond quickly and efficiently 24/7/365.

For more information:

Abuja Office	IGI House, Zone 4, Wuse, Abuja, Nigeria
Lagos Office	196B, Jide Oki Street, Victoria Island, Lagos, Nigeria
Email	sales@layer3.com.ng
Website	www.layer3.ng
Telephone	+234 9 782 2522, +234 1 280 5526