FORTINET

WHITE PAPER

# Say 'Yes' to BYOD

## How Fortinet Enables You to Protect Your Network from the Risk of Mobile Devices

## Introduction

Bring Your Own Device (BYOD) and consumerization of IT are all phrases that serve to encompass both the improvements in productivity offered by non-corporate owned devices such as tablets and mobile phones with the increased security risks that come with these devices. Many employees are already using their own devices for work. Furthermore, a recent industry survey indicated that nearly 75% of employees already use their own devices to access work related data.[1]

Another industry survey of information security professionals shows a different view – that mobile devices are one of the highest risks to the enterprise today[2]. With the current generation of workers seeing BYOD as a right and an industry of security professionals viewing mobile devices as one of their top concerns, finding the balance between policy and technology to enforce the use of personal devices is challenging. This paper will explore some of the benefits associated with BYOD and how Fortinet allows you to achieve them while addressing some of the key concerns around deploying BYOD. Finally, this paper will explore a network-based approach to BYOD and why it is the best place to perform BYOD enforcement.

## Challenges Associated with BYOD

There are many intuitive advantages to BYOD -increased productivity, lowered costs, and improved employee acceptance. While these benefits are appealing, there are many serious challenges associated with deploying a secure BYOD environment, including loss of control, potential loss of data, and lack of consistent policy enforcement. The challenges associated with BYOD can force an organization to rigorously evaluate its security posture and infrastructure. Organizations have to consider their response to each of the following challenges:

### Loss of Control

Many employees have found that mobile devices often do not deliver the same strict policy enforcement capabilities as desktop devices. This policy gap enables many employees to use their mobile devices to access applications and content that is denied by standard corporate policy, such as video streaming. With mobile devices offering an easy way to bypass the limits normally imposed on them, users are putting a strain on the corporate network and exposing it to additional risk of compromise.

### Increase Potential for Data Loss

With devices operating outside the confines of the traditional brick and mortar enterprise, the potential for data loss increases significantly. The threats to mobile users include the risk of malware infection, inadvertent or malicious sharing of critical business data or the devices being lost or stolen. Additionally, rogue wireless networks exist in the public with the sole purpose of stealing unprotected data.

### Inconsistent Security Policies Across Devices

Another challenge for organizations looking to secure mobile devices is the inconsistency of policies across different devices. For every device manufacturer and version of the mobile operating system, there is likely going to be differences in what policies can be applied. Figure 1 shows the fragmentation of the Android operating system by version. Each version operates slightly different. Paired with the variety of hardware vendors in the market (figure 2) it is easy to see how the problem quickly compounds.

---

1 http://www.fortinet.com/press_releases/120619.html

2 http://www.isc2.org/workforcestudy

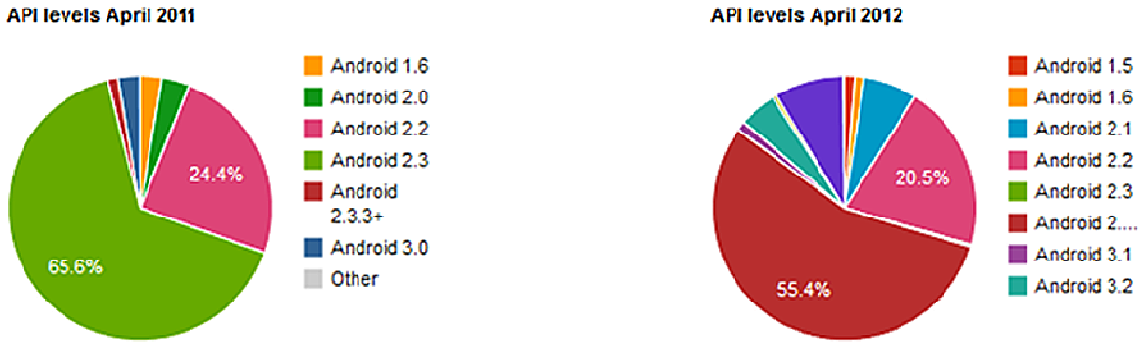


**Figure 1 - Android deployments by OS version**[3]

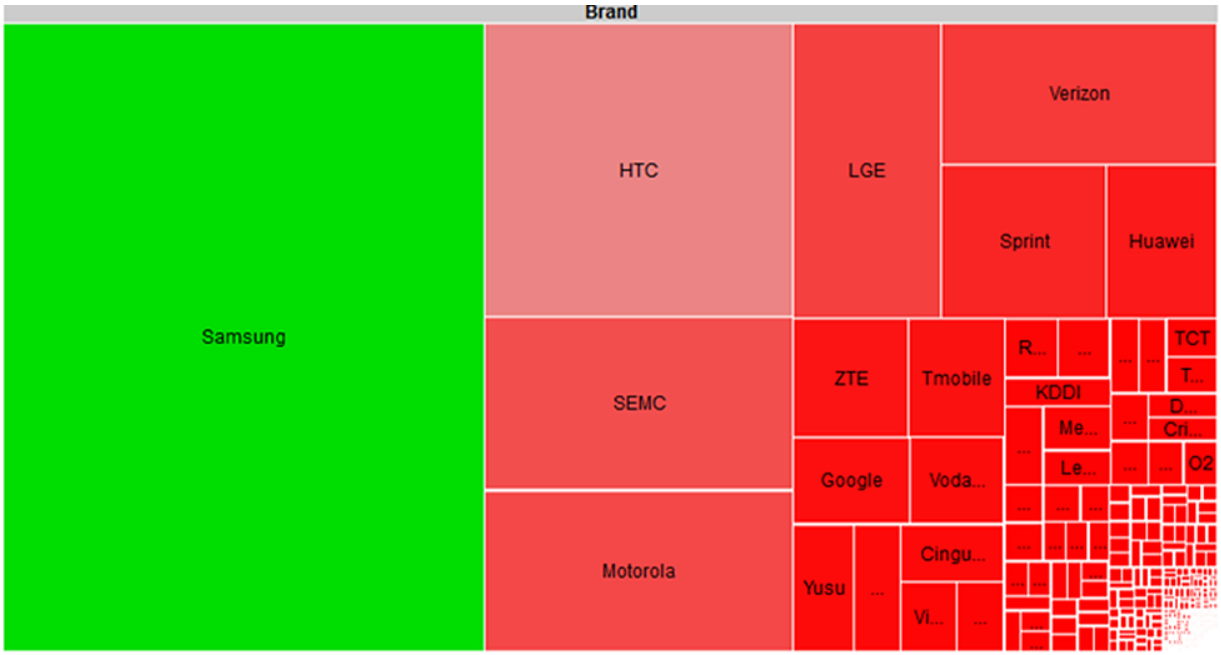


**Figure 2 - Android deployments by OS manufacturer**[4]

On top of the challenges of device market fragmentation, organizations also have to contend with device jailbreaking. Jailbreaking (or rooting) is the bypassing of manufacturer limits on a device, allowing users root access to the file system and giving users the ability to bypass inherent security policies on the device and install applications that are not inspected or sanctioned by the organization and could be malware[5].

3 http://opensignalmaps.com/reports/fragmentation.php

4 http://opensignalmaps.com/reports/fragmentation.php

5 http://www.ciosolutions.com/what-is-jailbreakingrooting/

## The Limitations of Mobile Device Management

The risks associated with BYOD have fueled interest in Mobile Device Management (MDM) solutions. However, MDM is not a complete solution to BYOD challenges as most MDM clients are designed to address many challenges that are not security-related, such as:

- Software Distribution
- Policy Management
- Inventory Management
- Service Management

MDM allows policy enforcement on the mobile device itself and many solutions offer remote location/lock/wiping capabilities to protect against loss or theft. However, MDM solutions enforce policies differently based on the mobile device they are supporting resulting in inconsistent security coverage.

## Solving BYOD Challenges Using the Network

Given the level of fragmentation that exists in the mobile device industry as illustrated above, it should be apparent that solving the mobile security challenge will be difficult by relying solely on agents. There are simply too many operating systems, devices and hardware platforms to expect agents to exist for every device and for every agent to act the same way on every device. Even today, one can take five smartphones from five different handset manufacturers all running Android, install the same security suite on them and still have different levels of policies and enforcement available. This is unacceptable from a security standpoint and puts compliance with regulatory requirements at risk.

There are always going to be some organizations and users for which agents are necessary. The CEO might be carrying information that is detrimental to the future of the company. However, the primary objective for most organizations implementing BYOD is to grant easy, secure access to the network across the entire user base, not just a few key users. Security professionals cannot rely on agents alone to secure the complex range of actions inherent in mobile devices. There has to be another layer of security that acts as the final authority. Ultimately the network can answer three critical questions the endpoint cannot:

- Who are you?
- Where are you going?
- What data do you need?

The answers to these questions will vary according to who the end user is, how their role is defined and where they are logging in from and as a result, the network needs to have the final say to approve/deny what a user is attempting to accomplish. IT professionals should include network security as they create their mobile device strategy.

## How Fortinet Secures BYOD

Fortinet understands that there is no silver bullet to address the security challenges posed by mobile devices. Solving them requires a technology-driven, multi-pronged approach. Fortinet has a wide portfolio of products that can address the new threat vectors provided by mobile devices and enforce policy compliance for users, wherever they may be. Specifically, Fortinet provides secure mobility by protecting the network, the data, and the end user.

### The Power to Control the Network

The network is the core component of any organization. Any disruption to the network is a disruption of services for users and the business. Fortinet was created to effectively defend the network from a wide variety of threats and every Fortinet appliance provides advanced functionality including an industry-leading firewall, intrusion prevention, application control, secure remote access, and antimalware. Fortinet also provides unmatched control over the network by providing unmatched visibility, granular control of users and applications, physical and virtual appliances, devices for any size network, single pane of glass management, device- and user-based policy enforcement and many other features.

### The Power to Control Applications & Content

Next to the availability of services, the data is the next critical component for organizations. A loss of data can mean a violation of compliance mandates, the loss of critical intellectual property, and most importantly, the

loss of customer trust. Fortinet provides granular protection of an organization's most sensitive data through a variety of controls around application security, data loss prevention, and web filtering.

**The Power to Control User Behavior**

Finally, the mobile client itself is at risk from attack when off the corporate network. Fortinet secures mobile clients – laptops, smartphones, and tablets – and protects end users while they are outside the office. Fortinet has solutions aimed at the endpoint itself that allow for encrypted communications from any location, ensuring that users are communicating securely from wherever they are located.

## Conclusion

The potential for greater productivity and cost savings almost guarantees that the movement towards allowing employees to BYOD is not going away anytime soon. In order to secure their data and devices, organizations will need to look towards network-based solutions and not just wireless and agent-based solutions that claim to solve the BYOD challenge, as these address only part of the problem.

Fortinet's holistic, network-based approach to BYOD provides organization a cost-effective, unified solution. The Fortinet approach is straightforward and eliminates the many headaches associated with client management and interoperability of a variety of devices from different vendors. In other words, Fortinet gives organizations the power to safely and securely BYOD.



FORTINET

GLOBAL HEADQUARTERS
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE
Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784