Enabling Seamless & Secure Mobility in BYOD, Corporate-Owned and Hybrid Environments

Efficiently and Cost-Effectively Managing Mobility Risks in the Age of IT Consumerization
# Table of Contents

## EXECUTIVE SUMMARY

## MOBILE DEVICE VISIBILITY, SECURITY AND CONTROL

## EVALUATING BYOD DEPLOYMENTS

- Understanding the Security Risks of BYOD
- The Primary Causes of BYOD Security Risks
- Outdated Software
- Inability to Prevent/Enforce Installation of Specific Mobile Apps
- Consumerization of Cloud Storage

## EVALUATING HYOD AND HYBRID BYOD/HYOD DEPLOYMENTS

## MITIGATING MOBILE SECURITY RISKS

- Evaluating Device Ownership
- Creating Risk Profiles
- Relying on a Security Cloud

## CONCLUSION

## ABOUT ZSCALER
Executive Summary

Companies worldwide wrestle with the balance between providing employees the freedom to choose the mobile devices they prefer for gaining access to enterprise applications and data or issuing secure, managed mobile devices for accessing enterprise network resources—and many companies implement hybrid environments that support both employee-owned and corporate-issued mobile devices. Consumerization and the proliferation of mobile devices is here to stay, and a cloud-delivered security solution can allow organizations to effectively manage the cost, efficiency, productivity, risk and security implications of seamless mobile access to enterprise resources in Bring Your Own Device (BYOD), corporate-owned and hybrid environments.
Mobile Device Visibility, Security and Control

Enterprise IT security is undergoing a transformation brought on by the consumerization of mobile devices and cloud applications. Employees need seamless and secure remote access to enterprise information, but IT needs to safeguard enterprise resources and protect applications and data. The level of visibility and control over mobile devices is a tradeoff that has to be managed; the greater the central visibility and control over smartphones and tablets, the greater the protection of enterprise resources.

When it comes to equipping the workforce with mobile solutions, many companies are adopting BYOD policies, allowing employees to leverage personally owned mobile devices to access company resources, applications and data. But BYOD brings security challenges; the same smart phone that might have been used to visit a malicious website last night could be used to access the company’s network today, and users are increasingly moving enterprise files to consumer cloud storage services like Box and Dropbox. Centralized IT departments also face the challenge of enabling the productivity of mobile workers while protecting corporate data and defending against malware and rogue mobile apps.

Security concerns are driving some companies to assert tighter control over their mobile devices and apply Here’s Your Own Device (HYOD) policies where IT distributes mobile devices to employees. Other companies are implementing hybrid BYOD/HYOD policies that allow gradual migration to HYOD implementations so they can optimize visibility, security and control. Developing a strategy for managing security for mobile devices is more important than ever, particularly given the growth projections for smart phones and tablets. According to global research and advisory firm Forrester:

- By 2016, there will be a billion smart phones and over 760 million tablets globally
- 60% of mobile devices today are utilized for both work and personal use
- 52% of employees use three-or-more devices for work today

Evaluating BYOD Deployments

BYOD allows employees to connect their own devices to the corporate network, and it offers:

- Employee choice and a greater feeling of personal control
- Fewer device support issues for IT
- Potential cost advantages

With BYOD, employees can use their own devices to access email, intranets and corporate applications. Other aspects, such as cost of ownership, are still widely debated since no consensus exists that BYOD actually lessens the cost of ownership. Some market research even shows that BYOD may result in higher costs. For example, the Gartner report, Bring Your Own Device: New Opportunities, New Challenges¹ found that, “BYOD programs can reduce cost, but they typically do not”. Gartner cites a wide range of cost drivers, including:

- The increased costs of software, infrastructure and support for BYOD platforms
- The cost of file sharing, business applications and collaboration tools
- Low acceptance by the workforce of the BYOD model
- Higher international travel costs when devices and carrier plans could be more efficiently managed centrally

Understanding the Security Risks of BYOD

The enterprise has to carefully evaluate the security risks of BYOD deployments. The Gartner report, Three Crucial Security Hurdles to Overcome When Shifting From Enterprise-Owned Devices to BYOD listed security vulnerabilities, data leakage and privacy concerns as being the primary risks to BYOD. The user’s freedom in selecting the device type as well as the apps on it causes risks of potential leakage of sensitive corporate data.

The user is able to upload sensitive data to any website or cloud storage service of their choice without the enterprise being able to view, control or prevent the leakage. Users increasingly copy corporate data to their own personal cloud storage accounts, leaving corporate data vulnerable to leakage. The user is also solely responsible for maintaining the security of the device, such as keeping the device Operating System (OS) version up-to-date to protect it from exploits or hacker attacks.

Technologies like Mobile Device Management (MDM) allow enterprises to deploy their corporate apps and settings on the device, but largely leave the user solely responsible for keeping the device secure and up-to-date. MDM enables IT organizations to manage, provision and monitor mobile devices but it does not secure mobile devices from the sophisticated attacks being mounted against users today, and traditional security appliances were not built to secure the 3G and 4G cellular traffic from mobile device.

Newer technologies like corporate data storage within secure “containers” isolate corporate data from personal data. This provides for the security of the corporate data alone— independent of the personal settings and apps on the device. But MDM and container technologies are not security solutions; they are management solutions handling deployment and provisioning of corporate applications and data on a personal mobile device. Even if the enterprise were to observe malicious activity from an employee-owned app while the device was connected to the corporate network, in most cases the enterprise lacks the ability to forcibly remove or even concretely identify the offending app on the device. This results in malicious activity on corporate networks caused by employee-owned devices and their personal apps that are running on them.

The Primary Causes of BYOD Security Risks

There are three fundamental reasons employee-owned devices pose greater risks to corporate data than corporate-issued mobile devices:

Outdated Software

Out-of-date mobile OS software, plug-in software and app versions pose a baseline security vulnerability for all mobile devices. Only a fraction of mobile users upgrade their devices the day an OS update is released, and they’re usually the early adopters who prefer to be at the forefront of every new software release. These early adopters are typically followed by a “long tail” of users who upgrade their devices days, weeks or even months after the upgrade was initially made available.

In BYOD environments, enterprises lack the visibility needed to identify whether an employee-owned device is running the latest software releases, and they have no ability to enforce an update to ageing operating systems and applications. Updates of Apple’s iOS operating system software for iPhones and iPads are available to users the day Apple releases them. But the Android OS is fragmented, resulting in device vendors taking weeks or even months to qualify Google’s new OS versions and roll them into their distributions.

---

While Apple users upgrade relatively quickly, the distribution of Android OS updates results in multiple versions deployed and increased security risks. The chart on the left shows iOS versions a month after the release of iOS 6.0, and the chart on the right shows Google Android fragmentation as of January, 2013.

Meanwhile, older but not-yet-upgraded mobile devices are vulnerable to security threats addressed in well-publicized but not net available OS releases. Hackers exploit these vulnerabilities to target unsuspecting users whose devices suddenly become prime targets of phishing, spyware and other common attacks. Many such attacks trick the user or device into releasing sensitive information, such as:

» Device contacts
» Calendar information
» User credentials

Inability to Prevent/Enforce Installation of Specific Mobile Apps

Enterprises cannot prevent nor enforce the installation of specific mobile apps in BYOD environments because the device owner has control over all configurations. The device owner has access to the official app markets as well as unofficial storefronts where illegal apps are available for download. In early 2013, Apple announced that there had been over 40 billion apps downloaded from its App Store, with almost half of those downloads coming in 2012. Android’s leading market, Google Play, hit the 700,000 download mark in late 2012. The leading popular apps on these platforms are not developed by well-known software development companies but by third-party developers that make a living publishing mobile apps. The inability of enterprises to control the nature of apps installed on employee-owned devices results in an unmanageable, uncontrolled number of apps that get access to the corporate network and to critical internal enterprise resources.
**Consumerization of Cloud Storage**

Corporate data is no longer as tightly secured behind corporate firewalls in locked-down servers. Cloud storage and mobile apps have enabled employees to take corporate files and store them in personal cloud storage accounts, often without the knowledge of enterprise IT departments. Enterprises therefore lose control over the types of data that gets uploaded to public cloud storage services.

*Graph: Global Mobile Cloud Traffic*

![Graph showing mobile cloud traffic growth](image)

*Cisco predicts that mobile cloud data traffic will increase to 71% by 2016. Source: Cisco VNI Mobile Data Traffic Forecast, March 2012.*

**Evaluating HYOD and Hybrid BYOD/HYOD Deployments**

HYOD allows the enterprise to implement greater visibility and security than BYOD because IT can implement tighter device and application control. By issuing corporate-owned mobile devices, IT can gain full visibility into all traffic from mobile devices to secure enterprise resources.

Corporate-owned devices enable secure browsing on all networks at all times and provide the enterprise with maximum control for enabling seamless and secure mobility. But employees lose some flexibility in selecting their preferred phones and tablets, and the enterprise absorbs the costs of buying, distributing and centrally supporting and upgrading the mobile devices. Hybrid BYOD/HYOD deployments are options for companies that have BYOD in place but seek to migrate to the visibility and control levels of HYOD over time. In this scenario, employees with their own phones and tablets can be granted remote access to enterprise resources while new employees are issued corporate-owned devices. As BYOD phones and tablets reach end-of-life, they can be replaced with corporate-owned platforms—thus providing the enterprise with a gradual migration path to HYOD solutions.
Mitigating Mobile Security Risks

To mitigate mobile security risks, enterprises should have their mobile traffic secured, not only to detect and block malicious transactions but also to manage sensitive corporate data. The first step is to ensure visibility so an enterprise can see the mobile traffic on their network connecting to their corporate data and resources. There needs to be mobile app-aware visibility and reporting of the:

» Mobile traffic
» Associated users
» Types of resources

The next step is to complement visibility with the ability to secure and control traffic that may be malicious or non-compliant. This includes detecting and blocking advanced threats through the mobile browsers as well as application-specific threats such as malicious apps and apps that leak sensitive information over the network.

Evaluating Device Ownership

Mobile platforms differ substantially in their ability to allow traffic visibility purely based upon who owns the device. For example, for corporate-owned Apple iPhones and iPads there are feasible options for having all mobile traffic inspected by content security solutions. But for employee-owned iPhones and iPads, Apple disallows the same methods. Companies with flexible BYOD policies may not want to manage their users’ mobile devices. However, IT does need to ensure that all mobile traffic accessing the corporate network adheres to the organization’s security and compliance requirements. This requires the ability to enforce corporate policies, restrict mobile app threats and even enable granular app control policies such as restricting usage of unauthorized or illegal mobile app markets.

<table>
<thead>
<tr>
<th>Security Over Public Networks</th>
<th>Security Within the Corporate Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HYOD</strong></td>
<td></td>
</tr>
<tr>
<td>Apple iOS</td>
<td>Apple’s supervision mode and Global HTTP Proxy enable coverage over all networks (3G/4G/LTE and WiFi)</td>
</tr>
<tr>
<td>Google Android</td>
<td>▪ Standardize on a specific vendor, like Samsung and its SAFE devices ▪ Evaluate options with your MDM or security vendor ▪ Recognize that having a multi-vendor approach reduces your options</td>
</tr>
<tr>
<td><strong>BYOD</strong></td>
<td></td>
</tr>
<tr>
<td>Apple iOS &amp; Google Android</td>
<td>Content inspection not feasible</td>
</tr>
</tbody>
</table>

*Options for mobile security while on various types of networks (3G/4G and WiFi)*
The enterprise needs visibility into all mobile devices when the device is on the corporate network, and organizations with BYOD policies seeking to augment mobile visibility and protection beyond the corporate network to include all corporate browsing traffic need to install browsers that can maintain a persistent proxy connection to a cloud-delivered security solution to ensure continuous protection. Companies that prefer to monitor and protect their employees mobile devices at all times can deploy corporate-owned mobile devices or containers of corporate apps on employees’ personal devices. Corporate-owned devices like Apple iPhones and iPads or corporate apps in Samsung Knox containers can be configured to maintain a persistent connection to the security cloud, thus ensuring that they are continuously protected.

**Creating Risk Profiles**

IT can create risk profiles to evaluate whether to issue mobile devices or allow employees to select their own. Enterprises often start by building a list of questions on how the device will be used and what kind of information it will store, such as the following:

- What types of corporate data (email, documents, etc.) will reside on the devices of our employees? This includes data from all applications employees can access from their mobile devices. The more data that gets downloaded onto the mobile devices, the greater the risk.
- Are technologies like Virtual Desktop Infrastructure (VDI) cost-effective for mitigating the risks of data left behind on the device? VDI is neither inexpensive nor does it present a very user-friendly native app access interface.
- What business benefits of BYOD are we achieving now?
- What would be the cost/benefit of offering exactly the same device platforms as corporate-issued devices with corporate controls instead?

**Relying on a Security Cloud**

When analyzing alternative approaches to mobile security, it is important to recognize that solutions need to be available at a global level, without the need to backhaul mobile traffic to one-or-more company data centers. Appliance-based network security solutions were designed to protect static corporate networks, and routing mobile and remote traffic through these appliances often slows traffic to an extent that it ruins the user experience. Imagine the latency of having to backhaul traffic from an executive traveling in APAC all the way to North America. Unacceptable response times limit user acceptance of security solutions, and a mobile remote access solution requires a ubiquitous presence around the world.

Deploying and managing a global private security network is not economically practical, but a multi-tenant, cloud-delivered security solution can act as a checkpoint in the cloud, scanning all incoming and outgoing traffic between any device—anywhere in the world—and the Internet—to identify and block potential threats. A cloud-delivered security solution allows the enterprise to select BYOD, HYOD or a hybrid combination of both employee-owned and corporate-owned mobile devices while eliminating the delays of backhauling traffic to a central location for security inspection according to company policies.
Conclusion

A cloud-delivered security solution enables seamless and secure mobility in BYOD, corporate-owned and hybrid environments. With a secure cloud solution:

» In BYOD deployments, IT can gain visibility, security and policy control while the devices are on the corporate network, and there is secure corporate browsing on all networks at all times with employee-owned devices.

» In HYOD deployments, there is secure browsing on all networks at all times for corporate-owned mobile devices and IT can gain greater control over device security.

» In hybrid BYOD/HYOD deployments, companies can gradually migrate from BYOD to HYOD or can design and implement policies for supporting BYOD or HYOD selectively based on the needs of user communities within the organization.

A security cloud solution can provide protection from advanced security threats with granular policy controls for browser and app traffic, flag apps with privacy or security risks and maintain near-zero latency while transforming enterprise security and enabling seamless, secure access for mobile users worldwide.

About Zscaler

Zscaler is transforming enterprise security with the world’s largest security cloud built from the ground up to safely enable users doing business beyond the corporate network. Zscaler’s security cloud processes over 8 billion transactions a day with near-zero latency to instantly secure over 10 million users in 180 countries, with no hardware or software required. More than 3,500 global enterprises are using Zscaler today to simplify their IT operations, consolidate point security products, and securely enable their business for mobility, cloud and social media. For more information, visit us at www.zscaler.com.