Taking BYOD Too Far

How to avoid the pitfalls of striving for BYOD utopia
CONTENTS#

CONTENTS........................................................................................................................................... 2
INTRODUCTION......................................................................................................................................... 3
DEVELOPING A BYOD STRATEGY ........................................................................................................... 3
  IDENTIFY RESOURCES THAT PROVIDE MAXIMUM PRODUCTIVITY.................................................... 3
  SELECT THE DEVICES THAT SUPPORT MINIMUM SECURITY STANDARD........................................... 3
  SIZE RISK OF LOSS OF DATA.................................................................................................................. 3
  INVESTMENT SHOULD NOT EXCEED EXPECTED RETURNS................................................................. 4
  NON-FINANCIAL CONSIDERATIONS ...................................................................................................... 4
  TAKE ADVANTAGE OF NATIVE DEVICE SECURITY CAPABILITIES................................................. 4
     DEPLOYING A DIGITAL CERTIFICATE ON AN IPAD USING GLOBALSEN’S IOS SOLUTION........... 4
CONCLUSION............................................................................................................................................ 5
CASE STUDY: MULTI-FACTOR AUTHENTICATION TO CORPORATE GMAIL........................................ 5
INQUIRE ABOUT OUR MOBILE AUTHENTICATION SOLUTION............................................................ 7
ABOUT GLOBALSEN............................................................................................................................... 7
INTRODUCTION

By 2018, 70% of mobile professionals will conduct their work on personal smart devices and there will be more than one billion global BYOD users, according to research from Gartner and Juniper. It’s no wonder organizations are having trouble keeping up with the plethora of BYOD point products and Mobile Device Management (MDM) solutions that stream into the market-place on a regular basis with many claiming to address all use cases, device types, and security concerns. The truth is many of them can, but what is the price of striving for BYOD utopia? The opening up of all, or most corporate resources to employees accessing the private network using employee owned assets may indeed increase productivity, however organizations must examine the trade-off in terms of cost, privacy concerns, and IT distraction in doing so. As with most security solutions, organizations should pause before jumping into implementing invasive, expensive, and all-inclusive BYOD solutions and ask themselves does the investment I’m making in BYOD provide for a positive return?

This white paper suggests that organizations should focus on creating a BYOD strategy that focuses on only 2 or 3 corporate resources that provide maximum employee productivity. Coupled with productivity considerations, organizations must examine the risk associated with the data being requested, and finally select controls that provide a level of security sized with the risk of breach.

DEVELOPING A BYOD STRATEGY

IDENTIFY RESOURCES THAT PROVIDE MAXIMUM PRODUCTIVITY

Let’s face it; the lure of BYOD began with the idea of employees using non-company provided devices to work remotely and often outside normal work hours. Cost savings associated with devices, monthly plans, and extended unpaid work hours produced an attractive proposition. All employees asked for in exchange was the choice of device.

However, the reality is most employees are satisfied with having access to applications, networks and resources that they most frequently use to stay productive, so why develop a BYOD strategy that attempts to address rarely accessed resources that can wait until the user has access from a company sanctioned and issued device. Three such commonly requested resources are:

1. Wi-Fi
2. Corporate Email
3. Virtual Private Networks (VPN)

SELECT THE DEVICES THAT SUPPORT MINIMUM SECURITY STANDARD

Accept that smart phone devices are in varying states of security and therefore your BYOD strategy might not be able to immediately accommodate all types of devices. If for example, you establish client-authentication using digital certificates for employee/device credentialing, there may be some devices or older operating systems that might not support (or easily support) PKI technology. However, if 70% of your employee base is using iOS, Android devices running O/S 4.3 and higher, or Blackberry devices, you might consider opening up networks using digital certificates to supported devices knowing that most older devices will likely be upgraded or replaced within 12 to 18 months.

SIZE RISK OF LOSS OF DATA

Accept that some data is so high-stakes because of its sensitivity, value or regulatory nature, that it should not be accessed via employee-owned devices. Piling on additional security measures may help protect the data, but at what cost in terms of employees’ device control and privacy rights? Organizations may think that imposing intrusive BYOD user agreements on employees will mitigate risk of employee abuse or sloppy handling of sensitive data, but relying on contractual (with little to no case law) methods as a data loss protection strategy provides little recourse when the data is regulated and your corporate reputation is damaged.
INVESTMENT SHOULD NOT EXCEED EXPECTED RETURNS

If the goal is to reap the rewards of increased employee productivity, then CFOs must take a hard look in terms of the investment needed to cover securing all or most data accessed by any number of devices. Let’s compare the cost of a Mobile Management System to implementing client-authentication to high access but low impact resources, such as corporate email using native client authentication capabilities.

<table>
<thead>
<tr>
<th>Hosting Enterprise PKI - 500 users</th>
<th>Annual</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
</tr>
<tr>
<td>MDM Solution</td>
<td>$6,250</td>
</tr>
<tr>
<td>Monthly device charge per employee</td>
<td>$19,500</td>
</tr>
<tr>
<td>Monthly hosting charge per device</td>
<td>$4,500</td>
</tr>
<tr>
<td></td>
<td>$24,000</td>
</tr>
<tr>
<td>Cost savings</td>
<td>$17,750</td>
</tr>
</tbody>
</table>

TAKE ADVANTAGE OF NATIVE DEVICE SECURITY CAPABILITIES

Many operating systems, such as iOS that both iPad and iPhone devices rely upon, have native capabilities that when used in conjunction with PKI services like GlobalSign, make provisioning digital certificates safe, easy, and cost – efficient. Below is an example of the user experience when installing a digital certificate using GlobalSign’s Enterprise PKI platform that leverages the SCEP protocol for easy over-the-air enrolment.

DEPLOYING A DIGITAL CERTIFICATE ON AN IPAD USING GLOBALSIGN’S IOS SOLUTION

**Step 1:** End user receives an email onto their iPad and clicks on an enrollment link. User enters a one-time certificate pick up password provided by their administrator to start the installation process.

**Step 2:** GlobalSign generates a SCEP request this is accompanied by either the GlobalSign default iOS configuration profile or a custom iOS configuration profile created using Apple’s Configuration Utility and uploaded into GlobalSign’s management platform. This profile is pushed out to the iPad associating the certificate with any special settings associated with the profile (settings ranging from VPN, Wi-Fi, and passcode rules can be added and pushed out with the profile as part of the certificate enrollment.)

NON-FINANCIAL CONSIDERATIONS

Financial considerations aside, organizations must be mindful of both user and IT administrator reactions to overly invasive BYOD strategies and policies.

**Employee privacy and moral:** Overly restrictive User Agreements that force employees to relinquish devices even temporarily, disable “apps” such as YouTube, and or wipe some or all contents are likely to receive a negative reaction since they are the ones footing the bill. Privacy concerns are heightened when devices share personal data such as pictures and personal contacts.

**IT distraction:** IT budgets are tight enough maintaining corporate furnished IT assets, let along supporting multiple device types and O/S versions. Employees agreeing to stringent user agreements may rightfully have the expectation that if something goes wrong with their device in terms of network access, then immediate troubleshooting and fixes will be made available. This may frustrate IT workers whom are tasked with focusing on core systems and may not be familiar with the particular device in question.
CONCLUSION

Today’s realities surrounding the current state of device technology, the absence of tried and legally tested BYOD user policies and lack of and/or desire for full control of employee owned devices suggests BYOD should be limited to access control of low risk data. Any attempt to adopt greater security measures into one’s BYOD strategy invites costly headaches for all involved. Therefore, maximize productivity and minimize risk of data and employee privacy breaches by implementing a non-intrusive BYOD strategy that focuses on limiting access to low risk, yet high yield applications. This can be achieved by selecting devices that have security technologies built into their operation systems and ignoring the complex outliers. And finally, consider using digital certificates in conjunction with the native device security capabilities and eliminate the need for costly middleware. Stop chasing BYOD utopia and start reaping the intended rewards to IT consumerization.

CASE STUDY: MULTI-FACTOR AUTHENTICATION TO CORPORATE GMAIL

Accessing corporate email can safely be said to be the most demanded resource by employees as it provides the greatest productivity gains. Organizations can easily utilize the native capabilities of Google to require strong authentication using digital certificates. GlobalSign's Enterprise PKI is a zero footprint SaaS solution that allows for fast, inexpensive, and easy to deploy method to implement client-authentication to applications like Gmail. The following is a case study on how iPad users using GlobalSign ePKI for Mobile iOS Certificates were able to securely access corporate Gmail using digital certificates provisioned from GlobalSign’s ePKI service.

Authenticating to Corporate Gmail Using Digital Certificates

Google Apps for Business by default allows users to login via username/password. This can be a security issue for companies where users’ passwords can be attacked. Google offers alternative methods for accessing their services to enhance security as well as improving the user
experience. Using the SAML Single Sign-on Service (SSO) for Google Apps web based applications, organizations can implement strong authentication using native capabilities found in many devices. The user experience is depicted below.

1. User signs into Gmail.

2. After successful authentication with email and password, user is prompted to present their digital certificate by clicking “Continue”.

3. User selects appropriate digital certificate that was earlier provisioned using GlobalSign’s certificate services.

4. User is granted access to Gmail.

As pictured in the steps above, utilizing digital certificates in conjunction with native services similar to Google App’s Single Sign on service can provide a secure, cost effective, and non-intrusive security measure to protect organizations’ sensitive data and keep employees productivity levels high accessing data outside the office.
INQUIRE ABOUT OUR MOBILE AUTHENTICATION SOLUTION

Call or email GlobalSign today to speak with a specialist who will help guide your organization toward a BYOD strategy and provide you with the tools to implement it.

For more information, visit https://www.globalsign.com/authentication/mobile.

ABOUT GLOBALSIGN

GlobalSign has been a trust service provider since 1996. Its focus has been, and always will be, on providing convenient and highly productive PKI solutions for organizations of all sizes. Its core Digital Certificate solutions allow its thousands of authenticated customers to conduct SSL secured transactions, data transfer, distribution of tamper-proof code, and protection of online identities for secure email and access control. Vision and commitment to innovation led to GlobalSign being recognized by Frost & Sullivan for the 2011 Product Line Strategy Award. The company has local offices in the US, Europe and throughout Asia. For the latest news on GlobalSign visit www.globalsign.com or follow GlobalSign on Twitter (@globalsign).

<table>
<thead>
<tr>
<th>GlobalSign Americas</th>
<th>GlobalSign EU</th>
<th>GlobalSign UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: 1-877-775-4562</td>
<td>Tel: +32 16 891900</td>
<td>Tel: +44 1622 766766</td>
</tr>
<tr>
<td><a href="http://www.globalsign.com">www.globalsign.com</a></td>
<td><a href="http://www.globalsign.eu">www.globalsign.eu</a></td>
<td><a href="http://www.globalsign.co.uk">www.globalsign.co.uk</a></td>
</tr>
<tr>
<td><a href="mailto:sales-us@globalsign.com">sales-us@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
<td><a href="mailto:sales@globalsign.com">sales@globalsign.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GlobalSign FR</th>
<th>GlobalSign DE</th>
<th>GlobalSign NL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tel: +33 1 82 88 01 24</td>
<td>Tel: +49 30 8878 9310</td>
<td>Tel: +31 20 8908021</td>
</tr>
<tr>
<td><a href="http://www.globalsign.fr">www.globalsign.fr</a></td>
<td><a href="http://www.globalsign.de">www.globalsign.de</a></td>
<td><a href="http://www.globalsign.nl">www.globalsign.nl</a></td>
</tr>
<tr>
<td><a href="mailto:ventes@globalsign.com">ventes@globalsign.com</a></td>
<td><a href="mailto:verkauf@globalsign.com">verkauf@globalsign.com</a></td>
<td><a href="mailto:verkoop@globalsign.com">verkoop@globalsign.com</a></td>
</tr>
</tbody>
</table>