The Definitive Guide to **BYOD**

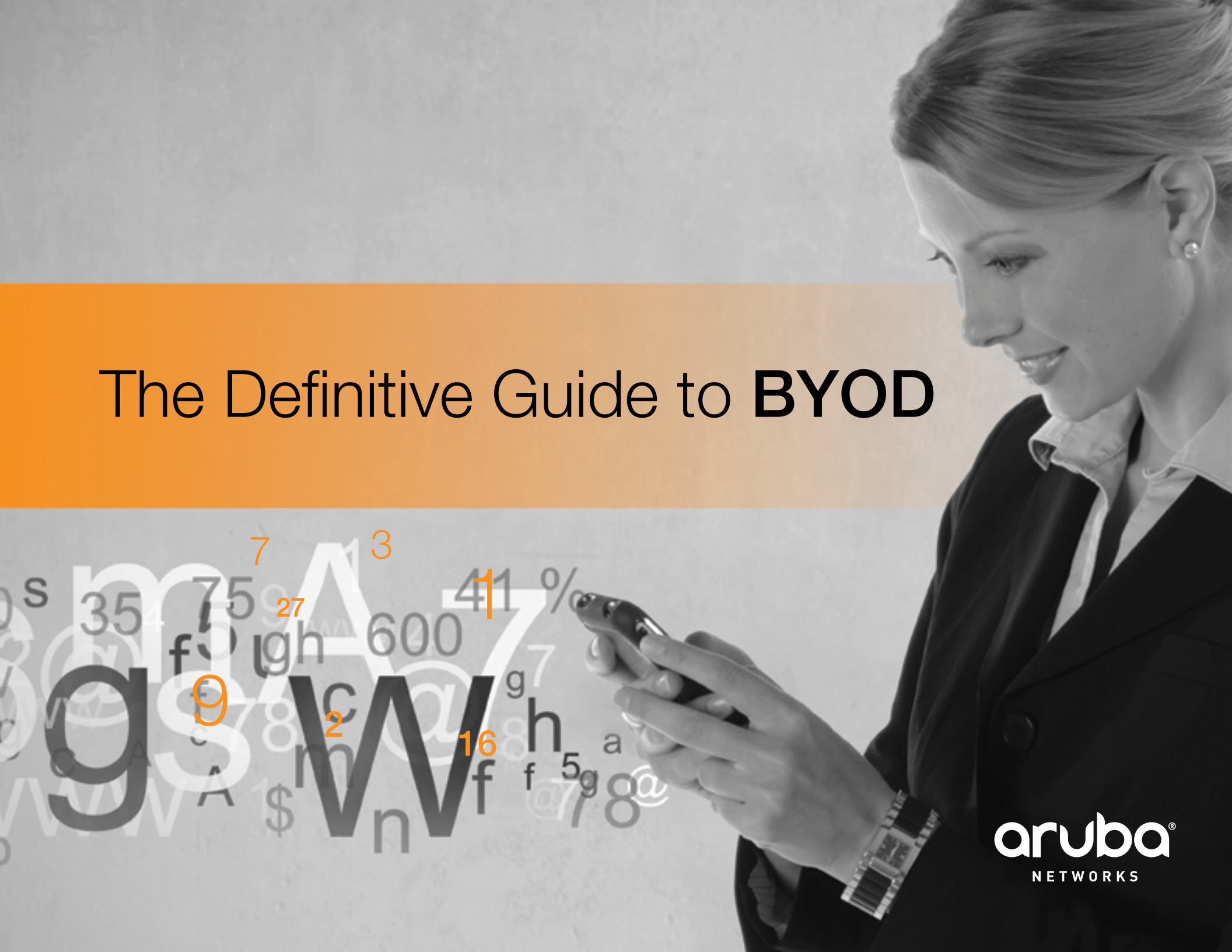


TABLE OF CONTENTS

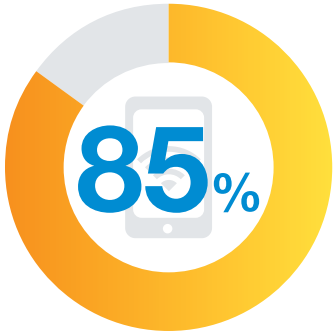
WHAT BYOD IS…AND WHAT IT ISN'T

BYOD – or Bring Your Own Device – is what happens when your employees or students or guests use their own personal smart phones and tablets for work. They bring their own mobile apps… security risks… privacy demands…with the intent to connect to your enterprise. And they expect you to make it work.

Because it's their *own* the device, uniformity goes out the window.

You're not handing them preconfigured devices to connect to secure enterprise networks, with work applications preloaded, and all administrative privileges pre-vetted by your IT staff. And you can expect that these devices take the path of least resistance to connect; whether that's your secure network using existing credentials or the guest network.

BYOD means that hundreds or thousands – or tens of thousands – of essentially *rogue* devices are interacting with your organization's confidential data and coming into your buildings every day…and it means that you need to come up with a plan that protects your confidential data and is transparent to users.



According to IDG Research Services, **85 percent of organizations** allow employees to bring their own devices to work.

WHY SHOULD I CARE?

Because all those users with their personal mobile devices are incredibly valuable to you. They're your brain trust…your engine…your heart and soul.

And they want to work the way they want things to work.

BYOD – done right – lets them do that. It can unleash new levels of productivity and operational agility. It let's your employees work with the technology that they're most comfortable with and that suits their exact requirements.

However done incorrectly, BYOD also opens your organization up to new levels of security vulnerability which destabilizes your carefully thought out plan. Not to mention bogging your organization down in hours and hours of helpdesk calls.

So, you care because you want to know how to best exploit the opportunities of BYOD while mitigating the worst of the threats. And we hope these few pages will help you with that.

BYOD – THE BIG PICTURE

1 2 3 4 5 6 7 8

- WHAT IS THE IMPACT OF BYOD?
- WHO'S GETTING THE MOST OF IT…SO FAR?
- WHAT DO THE ANALYSTS SAY ABOUT IT?

WHAT IS THE IMPACT OF BYOD?

In their 2012 "Worldwide Business Use Smartphone 2012-2016 Forecast Update," analyst firm IDC forecasted that, by 2016, worldwide shipments of smartphones will reach 480 million, with **65%** being used in bring-your-own-device environments.

- Instead of sharing a laptop in class, a third-grader checks in to her own reading assignment on her own personal tablet.
- A project coordinator accesses a corporate database for decision support – from his daughter's soccer game, using his iPhone.
- A marketing manager turns around a same-day niche opportunity – from his personal iPad mini, while in a staff meeting.
- An executive responds to a strategically critical email from the Shanghai office – on his Android Fire.

Thousands of times a day, these opportunities crop up –without BYOD, they would go unnoticed, unexploited, undeveloped. The opportunity costs are virtually infinite.

But then, actual costs can also add up as well. Tech support is bombarded with requests for configuration assistance and complaints about unreachable assets. Your enterprise-management team is scrambling to either validate third-party mobile apps or to develop new ones in-house that make these devices more usable.

There are also costs associated with beefing up your security infrastructure. And how do manage and control the way these devices and apps are used in your organization?

Finally, there are costs associated with the additional Wi-Fi capacity these devices demand. Your network was probably designed for about one Wi-Fi capable device per user, not three.

An effective BYOD solution brings optimum balance to this supply-demand equation.

WHO'S GETTING THE MOST OF IT…SO FAR?

There isn't an industry – or a corner of the globe – that isn't putting the mobile revolution to work for them. Here are a few examples of what they're doing to accommodate BYOD.

Enterprise

Everyone wants to stay connected to the office now. So enterprises are leveraging authentication methods and policies they currently use for IT-managed laptops, and extending them to personal devices. BYOD has shifted the security paradigm though: from managing every aspect of the device, to just managing enterprise apps and data, such as email and attachments.

Healthcare

Given all of the sensitive information and regulatory requirements at hospitals, it may be the last place you might expect BYOD to be embraced. However, a growing number of doctors and staff are using mobile devices for tasks such as patient monitoring, asset tracking, and consultation.

(continued on next page)

WHO'S GETTING THE MOST OF IT…SO FAR?

(continued from previous page)

By actively managing and securing BYOD for employees and guests, hospital IT teams can ensure compliance for HIPAA and audits while mitigating privacy concerns – while also accommodating patients, and their visitors, that want to use the hospital's guest network.

Education

Higher education practically invented BYOD. Colleges and universities have had to support student-owned devices for many years and have done an excellent job leveraging BYOD to transform the teaching and learning environment. Now, these same institutions are extending BYOD to faculty and staff.

In K-12, schools are providing shared resources and allowing students to bring their own device to support 1:1 student to device initiatives. IT needs a simple, secure, and easy solution that lets everyone self-register their devices and have access to school resources, regardless of what they're using. There are often content licensing implications that need to be considered if curriculum or testing and learning apps are made available to student's personal devices.

Retail

Retail spaces are completely transforming as a result of mobile devices. While most of these devices used by staff are issued by IT - such as iPads for mobile point-of-sale (POS) - there is a growing trend to also allow BYOD in stores for certain employees.

But the big story for BYOD in retail is for shoppers. Armed with smartphones, shoppers are price checking and reading product reviews while in the store – a Google/Think Mobile survey found that 77% of all smartphone users browse while shopping.

Wi-Fi networks can gather information about shoppers; improving the customer experience with real-time product information and special promotions to establish long-term social media connections.

WHAT DO THE ANALYSTS SAY ABOUT IT?

Basically, the analysts can see the writing on the wall. Here's a representative sample:

"Gartner expects the number of smartphones and tablets purchased to jump from 821 million in 2012 to 1.2 billion in 2013 as more of these devices invade workplaces around the globe."

—Carolina Milanesi, Gartner, Inc.

"You can look at BYOD as taking control away from IT or as an opportunity to mobilize your entire business. Accept that BYOD is happening and build a plan around it – how to manage it, how to secure it, how to get apps to devices."

—Maribel Lopez, Lopez Research

More than half of North American and European companies are developing BYOD programs in response to workforce demand.

—Forrester Research

WHAT QUESTIONS SHOULD YOU BE ASKING RIGHT ABOUT NOW?

1 2 3 4 5 6 7 8 9

- WHAT ARE THE OTHER CIOS AND IT MANAGERS ASKING?
- IS BYOD FOR EVERYONE?
- AND DON'T FORGET…

Many organizations are entirely reactive to BYOD, responding only as pressure from users increases. The reality is, most are allowing some form of BYOD today without any safeguards.

Cost, complexity and immaturity of the technology to secure BYOD are justification. But doing nothing is a risky game and, thankfully, technology has caught up.

It's time to plan your strategy and start gathering information. Start by asking about the number and type of personal mobile devices on your network. What impact BYOD is putting on your network and security resources.

In fact, let's see what others are asking.

WHAT ARE THE OTHER CIOS AND IT MANAGERS ASKING?

As you might imagine, the primary concern is with protecting corporate assets. So the main question is: *"How do I secure corporate information on a device we don't own?"*

The next major concern is about process, taking both organization and user concerns into account. The question here is *"What steps are necessary to address employees' BYOD privacy concerns while still addressing ease-of-use and security issues?"*

Next, you need to think about the impact to helpdesk and other operational resources. You should be asking *"How do I support BYOD without a budget increase or without additional*

IS BYOD FOR EVERYONE?

headcount allocated to the helpdesk?" and *"How much time and effort will it take to get all these BYOD solutions stitched together and working seamlessly?"*

Finally, there are cultural issues, particularly for the organization that still restricts mobile access to corporate-owned devices. From them, we're hearing: *"How can I loosen my grip so that my employees can use these devices for tasks that aren't confidential or for personal use?"*

This last one is actually an intriguing dilemma. Just as you might begin allowing employees to use corporate-issued devices for personal use, emerging privacy laws may hamper your using traditional security measures for BYOD, such as tracking of devices, visibility into personal data and installed applications or wiping a user's data.

BYOD doesn't discriminate on the size of an organization. Even small organizations will need to support personal devices and the daunting data-protection mandates.

The needs of an enterprise, however, can be quite complex, depending on its geographical layout, the sensitivity of its data, and how varied the needs (and consequent number of access levels) are of its users.

Bigger organizations also typically have a greater numbers of users who travel or are located in different physical locations. The more mobile and dispersed an organization, the more that personal devices become a necessity for keeping everyone connected – with both their colleagues and their lives at home.

And don't forget…

- What is the role of policies…how much do I control usage?
- Will I need new infrastructure?
- What do I do about mobile apps?
- What about corporate data…. how much risk am taking on?

We'll address all of these questions and more. But let's begin with the most obvious question: *Where do I start?*

WHERE DO I START?

2 3 4 5 6 7 8 9

- START BY NARROWING YOUR FOCUS
- CONSIDER YOUR CHALLENGES
- WHAT EXACTLY DO YOU LOSE IF YOU DON'T MOVE TO BYOD?

START BY NARROWING YOUR FOCUS

BYOD can be an awfully wide playing field. So, cut it down to manageable size: define which challenge you're trying to solve first. Is it security? Is it operational efficiency? Are you just trying to establish reporting and audit capabilities in the face of upper management demands?

Once you've established your primary challenge, narrow it down some more.

For instance, if security is the concern, is your objective to differentiate access to the network, applications and content if the device is personal versus IT-issued? Or is full tracking and reporting on BYOD use in your organization also required?

What about authentication? Will you require authentication of personal devices using device-specific certificates or is a MAC authentication satisfactory?

The good thing about narrowing your focus is that it allows you to develop that first building block of your overarching solution. Once you have that cornerstone in place, it becomes easier to build out the solution to address your secondary issues to create as comprehensive a BYOD program as needed.

Apple expects to sell **170 million iPhone 5's** in first year

CONSIDER YOUR CHALLENGES

As with many technology issues, the pace of change is one of your greatest BYOD challenges. How quickly will user and device numbers grow? How much will the demands on your help-desk grow and change as BYOD evolves? What types of mobile apps will users ask for?

You must develop a solution that can scale, be rolled out quickly, and adapt to a changing BYOD environment so that it's not already obsolete by the time it's implemented.

Balance is another critical challenge. You will continually have to walk the tightrope between the needs of the organization and the needs (and legal protections) of the individual user.

Finally, while a move to BYOD is inevitable, you need to consider if you are at that point now. What are your organizational readiness issues? More importantly, have you determined what exactly you lose if you don't make the move? For instance, how long will it be before user workarounds create an oversized problem for you?

The reality is, many organizations are supporting BYOD today not because they have a formal initiative, but because employees have figured out how to do it on their own. This can get ugly really fast.

WHAT EXACTLY DO YOU LOSE IF YOU DON'T MOVE TO BYOD?

"During the coming year, many companies will be faced with pulling off a balancing act between protecting company data and ensuring : BYOD users' privacy isn't trampled."

—Byron Acohido, USA Today

To put it bluntly: your ability to manage risk. As users increasingly combine work and personal applications on their devices, your management challenges grow more complex – and the chance that confidential data are leaked rises exponentially.

Devices are replaced, and lost or stolen, without IT being informed. Documents are not encrypted, but then stored in personal cloud applications. Jailbroken devices are infected and then connect to the network, which can have a detrimental effect on other users' data.

Given that application and data security is the top IT concern regarding BYOD, an emerging approach is to combine device and application management within the network access-management solution. In other words, an integrated approach.

Hold that thought. It will be important later.

ABI Research had estimated that by 2015 the number of these devices will have grown to over **2 billion** worldwide, a 300% increase from 2009

ARE THERE ANY OTHER CRITICAL ISSUES?

3456789

- WHAT ROLE DOES PROCESS AUTOMATION PLAY?
- WILL IT SCALE?
- SOME THOUGHTS ON DEVICE PROLIFERATION, POLICIES AND NEW INFRASTRUCTURE
- HOW DO I EFFECTIVELY ROLL OUT A BYOD SOLUTION?

WHAT ROLE DOES PROCESS AUTOMATION PLAY?

Given the relentless flow of new personal devices brought in by your users (because they've been replaced, lost or stolen), it's vitally important to automate processes within your BYOD program and enable as many self-help services as possible. For instance:

- **Device onboarding** – Don't do it manually. Make it intuitive and user-driven. This simplifies device registration and provisioning, as well as minimizing calls to the help desk.
- **Device profiling** – Make it consistent so manual intervention isn't needed. This ensures that policies based on device characteristics are properly enforced. User expectation can be properly set, with no surprises from false fingerprinting.
- **Usage management** – This ranges from automated access-differentiation (based on user role or device) to enforcement, which includes the ability to revoke access for one device without interrupting service for other devices.
- **Application management** – Ideally, you should be able to fully automate the process of distributing and updating mobile apps, while also giving users the ability to add optional apps through an enterprise app store. Application usage policies should be automated as well to quickly secure apps as the users' environment changes (e.g. network, location, time of day, etc.)
- **Device management** – Hand over basic device management functions to your users. This includes functions such as adding or deleting mobile devices from the network, connecting to printers and projectors and setting up shared relationships of personal devices with other users.
- **Guest access** – Take helpdesk and receptionists out of the equation. Let your users add and sponsor guests on their own. Give them control to add time expiration, issue passwords and control other guest functions that don't pose a risk to your or your organization.

WILL IT SCALE?

This is the same question you asked back when you put in your security solution for corporate-issued mobile devices, right?

Well…does it?

You're much better off if you have a platform that can scale to manage both IT-issued devices and BYOD. For instance, authentication against any device and user can be consistent which provides users a common experience. By managing everything from one place, you also ensure that policies and compliance are uniform across the entire enterprise.

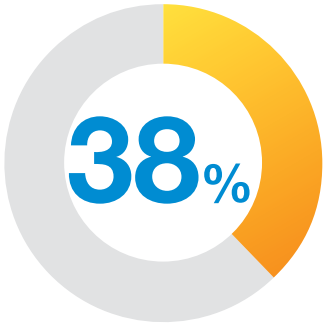
If your new BYOD solution is to be the standard across the organization to meet strategic objectives, it needs to scale for all types of employees and guests, across all types of applications and data, and across all geographies.

Also, it needs to consistently work across your entire network; whether a user connects to your wired and wireless network or roams to cellular 3G/4G and connects over VPN.

Your CIO must be able to show return on investment, which requires reporting tools that provide both visibility and a way to demonstrate where the solution has helped streamline processes for increased cost savings.

Most important, you want it to scale into the future – across a growing organization, across emerging technologies, across evolving business needs.

38 percent of companies expect to stop providing devices to workers by 2016.
—Gartner, May 2013



SOME THOUGHTS ON DEVICE PROLIFERATION, POLICIES AND NEW INFRASTRUCTURE

Apple sold more iPhones, iPads and iPod touches in 2011 than it sold Macintosh computers during the company's 28-year history.

—Gartner adoption of mobile learning

Left to their own devices

BYOD means dealing with a potentially infinite variety of device platforms and profiles – and you want to be able to automate management of this digital menagerie. Here's a typical hierarchy of approaches:

- **Minimize choice** – If you can limit users to a smaller pool of desirable choices, you can make management … manageable, offering automated configuration and onboarding services for the most popular models and platforms (Windows or Mac OS X for laptops, and iOS and Android for smart phones and tablets).
- **Device-centric controls** – This approach uses a specialized tool set that looks at basic characteristics of the device and installed applications in order to secure that device. Enforcement actions can be triggered based on factors such as the version of operating system changing and whether it has been jailbroken or contains any blacklisted applications.
- **Application and data controls** – This approach focuses on controlling just the applications and data that is relevant to the organization. Nothing else. It takes IT out of the device management business and lets them just focus on corporate assets.
- **Network access-centric approach** – This approach controls what personal devices can do on the network, limiting access to enterprise network resources and data

What's your policy?

As personal devices, and the possible data-loss associated with mobility, become greater security concerns, you'll want to enlist contextual attributes to help define more granular and focused enforcement rules -- which device will be allowed to reach which enterprise resources, at which times, by which user? And what about controlling the transferability of content and the use of certain mobile applications?

Start by determining whether or not personal devices should be allowed to connect to all network types (wireless, wired, and VPN). For instance, you may want to limit access for personal devices when connected over a VPN or when connected to a non-secure guest network.

With respect to controlling applications, do yourself a favor: make it an iterative process. Start with the commodity enterprise applications that serve the greatest number of people, like email, browser and collaboration tools.

The policies for these apps can lay the foundation for expanding to more mission-critical applications and a broader group of users. Develop a holistic strategic plan, with an eye on future moves as you build out policies that will gradually encompass your entire enterprise.

What is the pace of adoption of mobile apps? Does your organization develop its own apps? What apps do employees use to access most of their content? Answering these

(continued on next page)

SOME THOUGHTS ON DEVICE PROLIFERATION, POLICIES AND NEW INFRASTRUCTURE

(continued from previous page)

questions will help determine the appropriate application management tools and policies.

Infrastructure – new or used?

Your network capacity is critical. Can it support the number and diversity of devices that bombard it every day? And can it support the real-time multimedia-heavy applications that employees demand. Most of these demands will target your wireless network. Don't get pressured in to upgrading your wiring closet when mobility and RF is what really matters. Focus on where the bigger problem is.

Make sure you aren't exposed when a device roams from your Wi-Fi network to cellular. Data security needs to seamlessly adapt to a changing network environment.

Another key consideration is whether your existing infrastructure supports 802.1X, particularly for advanced security methods. It is still possible to support multiple user-authentication methods and BYOD with older equipment and methods, but not as straightforward.

If you can support advanced security on 802.1X and have a flexible policy-management system that supports multi-vendor requirements, then supporting BYOD is simply a matter of extending the connectivity provisions of your existing wired and wireless environments. This also ensures against disruption during a merge of organizations or as infrastructure upgrades happen.

You can then use the network access/BYOD solution to enforce whatever policies your existing infrastructure supports. This adaptability allows organizations to use a single BYOD platform regardless of which vendors networking equipment is used.

But be sure to keep your priorities straight: your strategic business needs should dictate how BYOD is deployed, not your network-access solution.

HOW DO I EFFECTIVELY ROLL OUT A BYOD SOLUTION?

The first step in an effective BYOD deployment is to include tools that automate repetitive user and IT processes. Equally important is to make sure that each IT stakeholder team understands their role in the deployment:

- **Network services** – For infrastructure configuration, rules enforcement, and policy management.
- **Security services** – For policy definition, agent and VPN rules, end-user awareness and usability.
- **Helpdesk services** – For implementation of usage policies and required troubleshooting information.
- **Desktop services** – For device management, application distribution and use.

In many organizations, these roles are converging, creating new roles and responsibilities for those managing mobile security and BYOD.

From the end-user perspective, onboard devices and connect to the network must be simple, regardless of how strict the policies. To this end, working with an existing identity store can prove invaluable, as will tools that easily identify a user device as they start onboarding.

Lastly, a proof-of-concept and phased deployment is recommended. This allows you to address the particular concerns of specific groups and gather feedback on policy effectiveness, end-user experience, and next steps for further deployment. Local and remote deployment testing should be considered.

Adoption of social networks is expected to grow rapidly among mobile users and by 2016 the number of mobile social-network users will reach **1.5 billion**. *—Gartner Hype Cycle for Wireless Devices*

READINESS CHECKLISTS

4 5 6 7 8 9

> THE BYOD LANDSCAPE: AUDITING YOUR EXISTING INFRASTRUCTURE

THE BYOD LANDSCAPE: AUDITING YOUR EXISTING INFRASTRUCTURE

The BYOD landscape: Auditing your existing infrastructure

One of your first tasks should involve using available planning tools to outline what you want to allow and disallow, and the nature of your BYOD work flow. These checklists should help you identify unique BYOD requirements for your organization.

Infrastructure preparedness

First, let's take a look at the current state of your infrastructure.

Access needs

- ☐ Number of Wi-Fi access points? _____
- ☐ Description of Wi-Fi equipment (model, 802.11 standards, age, authentication capabilities) _____

_____

- ☐ Number of Ethernet access ports? _____
- ☐ Description of Ethernet equipment (model, speed, power, age, authentication capabilities) _____

_____

_____

_____

- ☐ Description of VPN infrastructure _____

_____

_____

- ☐ IP addressing scheme (static vs. dynamic addressing)
- ☐ Description of WAN infrastructure _____

_____

_____

- ☐ Network topology considerations (number and type of local or remote facilities)_____

_____

Identity sources

- ☐ Type of identity stores (Active Directory, LDAP, SQL database, two-factor authentication) _____

_____

_____

- ☐ Location of BYOD solution and identity stores _____

_____

- ☐ Interaction with domains
- ☐ Authentication and authorization sources (user and device enforcement)

Device and content management

☐ Number and type of devices in your network _____

_____

_____

☐ Existing mobile device or mobile-application management infrastructure

☐ Virtual desktop infrastructure

BYOD preparedness

To narrow your focus on the best approach for your environment, the following points should be discussed and considered.

Network use policies

- Identity that matters to you (user name, title, group, department)
- Device type – model, OS version, familiarity (known or unknown)
- RADIUS accounting uses
- Device posture and health checks
- Other relevant device attributes
- Application usage attributes
- Conditional attributes (time, day of week, location, local user access vs. roaming users)
- User-driven device registration (Apple Bonjour-capable devices, game consoles, printers)
- Wireless and wired interoperability Redundancy

Device onboarding

- Automate on-ramping and configuration of end-user devices (laptops, smartphones, tablets)
- Use of certificates and unique credentials

(continued on next page)

Smart device popularity drives opportunity for mobile app stores which by 2016 will reach 310 billion downloads and **$74 billion in revenue.** *—Gartner Market trends Mobile App Stores*

(continued from previous page)

Device onboarding

- Built-in certificate authorities (CA) with customizable certificates
- Ability for IT or user revocation and deletion of certificates for lost or stolen devices
- Use of contextual data to build policies (MDM attributes, user, device type)
- Limits for number of allowed devices per user

Mobile device management

The following checklist will help you identify your device management needs and the available MDM capabilities that can address them.

- Device inventory (tracking of device ID, hardware model, firmware version, wireless adapters)
- Classification of devices (known, unknown, OS versions)
- Using device profile information (visibility only or policy-based)
- Treatment of unmanageable devices (printers, IP cameras)
- Devices required for full management (model, ownership, corporate-issued vs. personal)
- Physical tracking (location-based GPS support)
- Integration (other managed assets such as laptops and phones, integration of mobile device records into a common database, required policy management system)
- Remote find-and-wipe capabilities
- Network authentication (integration with enterprise directories, network-disconnected authentication)
- Password policy enforcement (PIN codes and failed-attempt actions)
- Connection whitelists and blacklists
- Audit and compliance (proof that devices comply with stated policies and industry privacy regulations)
- Software versioning
- Application whitelists and blacklists
- Device data backup
- Remote control
- Telecommunications expense management
- Enterprise app store

Mobile application management

BYOD has evolved to include the management of mobile applications, which is now considered an essential best practice.

- Software packaging (bundling of related applications)
- Application distribution (software and updates downloaded from public app stores like Apple iTunes and Google Play or pushed transparently to managed devices from a private enterprise app store)
- Change control (application updates and policy changes do not cause pain to users or weeks to implement)
- Application security (built-in, on-device and in-motion encryption with per-app VPN capabilities)
- No agents required
- Personal and enterprise data are kept separately on a single device

- No physical tracking (ensures privacy and compliance)
- Per application policies (prevent cut-and-paste between enterprise and personal apps, location, motion, app locking)
- User self-help portal (cost-effectively shifts administrative tasks away from IT)

Guest access

The better BYOD solutions include full-featured visitor management capabilities. The idea here is to lower demand on IT resources by automating tasks and allowing users to self-provision guest access.

Management requirements

- Sponsors (non-IT staff or self-registration capabilities)
- Management of the sponsor experience (differentiated privileges, multiple branded portals)
- Ability to create guest credentials from personal devices
- Policies for classes of guests (day visitors, contractors, temporary employees)
- Policies for usage rights and restrictions (bandwidth, length of stay, day of week)
- Audit of guest activity
- Integrated posture checks (with remediation and quarantine)
- Hotspot scalability
- Ability to charge or offer promo codes
- Centralized guest management across multiple locations
- Advertising (enterprise messaging or retail-level campaigns)

Guest user experience

- Branding, familiar look and feel
- Network usage messaging
- Simple device-connection workflow for new user
- Transparent device connection for existing user
- Credentials received via SMS and email
- Complimentary hotspot access

Administration

End-to-end clarity and control is required to effectively manage mobile users, devices and apps for BYOD. By end-to-end, we mean visibility across multivendor, multisite wired and wireless networks.

- Reports and analysis required in real time
- Automatic alert capabilities
- Reporting requirements (employ search criteria like user, IP address, device type, MAC address)
- Required historical reports and logging
  - Authentication history
  - Device compliance
  - Policy events
  - Application adoption and usage
  - Other_____
- Interface to external syslog or SNMP servers
- Command and control for violations
- Differentiated helpdesk access

Gartner estimates that tablet production will grow from slightly fewer than 120 million units to more than 370 million units in 2016. Smartphone production to increase from approximately 650 million units in 2012 to more than 1.3 billion units in 2016

—Gartner adoption of mobile learning

ASSESS YOUR OPTIONS

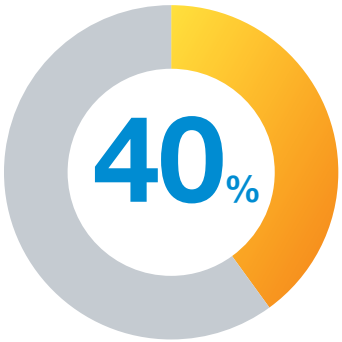
5 6 7 8 9

- WHAT ARE MY ACCESS OPTIONS?
- WHAT ARE MY AUTHENTICATION OPTIONS?
- WHAT ARE THE AVAILABLE ENFORCEMENT METHODS

WHAT ARE MY ACCESS OPTIONS?

Differentiated access to accommodate diverse user groups and needs is the critical factor in assessing your access-solution options. Many early BYOD initiatives didn't allow for differentiated access and, as a result, they would suffer from insufficient visibility and potential bandwidth scarcity.

Differentiated access is built on the practical working concerns of different user groups. For instance, different functional departments in an organization are given access to different resources and applications. Device classes, such as "BYOD" may be given different access privileges than say "corporate issued."



40% of business say BYOD is the main concern when developing and managing smartphone/tablet apps and devices
—Forrester – Prepare for connected enterprise

Differentiated access may also mean controlling the number of devices a user can bring to work. For instance, executives or sales personnel may be allowed to onboard up to two personal devices because high mobility, along with constant customer interaction, are expected.

Office-based employees, on the other hand, may be limited to one personal device because they are likely to spend most of their time on a corporate-issued computer.

Visitors are also a discrete group with their own access needs. A guest-access solution can be used to separate guest traffic, customize the experience for each user and provide visibility on who is connecting. Blended access solutions of this nature also give your IT staff the necessary data for adjusting bandwidth requirements, as well as for planning purposes and user-based network audits.

WHAT ARE MY AUTHENTICATION OPTIONS?

As in our discussion of infrastructure, one of the key functions here is being able to support 802.1X.

If you can deploy enterprise-mode wireless access or Wi-Fi Protected Access (WPA2) using 802.1X authentication, you can increase security and support multiple EAP types and device certificates. In environments where personal devices are being used, this encrypted authentication takes advantage of the AAA services offered in best-of-class BYOD solutions.

For laptops, with their wired capabilities, 802.1X lets you designate a user's access privileges regardless of where they connect. And policies can be established to automatically enforce differentiated access rather than requiring the IT staff to manually configure switches.

Along with setting up 802.1X variables on the devices, the BYOD solution should also allow you to install your RADIUS server's CA and any required agents or applications, regardless of device type. The goal is for users to easily establish authenticated connections to your network without IT intervention.

WHAT ARE THE AVAILABLE ENFORCEMENT METHODS?

More than half of information workers, 53%, use their own personal devices for work; install unsupported software; or use unsupported Internet-based services like Dropbox, Skype, Twitter, or Facebook to help them do their jobs.

—Forrester – Prepare for connected enterprise

Many organizations have already invested time and energy to create network segmentation and security with VLANs, stateless access control lists (ACLs), and firewalls.

While the network-access solution should leverage existing infrastructure, equipment that supports role-based policies should also be considered. With BYOD, the likely increase in both remote connections and high-bandwidth applications like video demands more granular enforcement.

The advantages of utilizing more than VLAN steering and ACLs for dynamic, per-user enforcement include:

- Per-session stateful firewalls with ACLs.
- Defined bandwidth limits and permit lists.
- Quality of service (QoS) and type of service (ToS) priorities.
- Captive portal redirection across network infrastructure.
- VLAN assignment.

The interdependence of policy and enforcement are really important and benefits include your ability to assign different roles based on contextual attributes such as user role, device type, application type, location and so on. At some point, the type of device may then drive fundamental operational rules for how enterprise applications are then distributed and used.

More than half of information workers, **53%**, **use their own personal devices** for work; install unsupported software; or use unsupported Internet-based services like Dropbox, Skype, Twitter, or Facebook to help them do their jobs. *—Forrester – Prepare for connected enterprise*

THERE HAS TO BE A WAY TO LOOK AT THIS HOLISTICALLY

6789

- THE ROLE OF MDM
- HOW IS MDM CHANGING?

THE ROLE OF MDM

The first generation of mobile device management (MDM) has been great – for managing corporate-supplied devices…and when privacy of employee-owned content and applications aren't at issue. The shortcoming of MDM is that it is designed to take the entire device under management and as such has trouble balancing user needs with enterprise needs in true BYOD situations. A few things you should take into consideration when looking at MDM:

- **Employee privacy** – MDM gives you complete visibility and control of a user's personal mobile device, including private information such as GPS location and installed personal applications. In fact, some of this information, like location, might be illegal for you to have access to. Violating user privacy not only has liability implications, but it could also alienate your user and cause them to bypass MDM controls
- **Selective Control** - With MDM, the enterprise often controls all content on the device. What you really want is the ability to differentiate control between corporate and personal data. For instance, you should be able to lock or wipe specific corporate content on the device without impacting a user's own data.
- **Data protection** – Some MDM solutions provide data encryption on the entire device but very few add encryption across the network. This puts both the data and the organization at risk due to breaches and/or compliance violations. The preferred method is to add encryption to applications and content that need it and to enforce encryption of this data on the device (at rest) and across the network (in motion).

- **Automated services** – MDM solutions offer very few self-service capabilities to users, thus increasing the load on IT helpdesk resources. You should look for solutions that empower users to take actions such as create guest credentials, self-register devices or easily discern enterprise apps and associated policies.
- **Network security** – using device posture information such as jailbroken status or settings violations cannot impact network security decisions. And network events such as congestion or device roaming can't impact device policies. Most MDM vendors will have you buy a separate Network Access Control (NAC) system to control BYOD on the network.

"Networking pros will have to figure how to create infrastructure that makes **WLAN a primary way to connect,** not just a nice-to-have add-on." *—Forrester Networking predictions 2013*

HOW IS MDM CHANGING?

Consumers of popular VoIP services like Skype also want to extend that capability to their mobile phones. VoIP could add 20% to 40% in additional capacity on all-IP networks, which could cut the costs of supporting wireless voice services, and over-the-top providers will all have low-cost voice apps that will take advantage of all-IP networks.
—Gartner Hype Cycle for Wireless Devices

The focus of MDM's most recent evolution is known as containerization: a separate zone is carved out on the user's device, in which authorized enterprise apps and data reside, with policy controls applying only to the container's contents, not the entire device. This space may be visually separated for the user but doesn't need to be.

It's like having two devices in one – an employee device with personal preferences, applications and data; and a parallel universe with all the corporate apps and data. Three different containerization examples are:

- **The sandbox** – Enterprise applications and data are put into an encrypted space, or folder. But application developers must write to a custom specification that supports the proprietary folder environment.
- **Virtualization** – Multiple virtual machines run simultaneously. A hypervisor allows IT to securely manage the enterprise's virtual domain, while the user manages the personal virtual domain.
- **The wrap** – Each application is dynamically wrapped with a layer of security and policy. Developers don't need to write and compile each app for a specific enterprise *sandbox* to maintain a consistent look and feel for users.

While each approach has advantages, the wrap approach lets you quickly update a policy for – or delete access to – individual apps. For example, any enterprise app can be configured to limit access based on time, location, device movement, or jailbreak status. It also provides the most transparent user experience with many automated policy controls.

There is, however, an emerging approach that lets you wrap an app, and also eliminates the need to manage a user's personal apps and data. This approach integrates device and application management within the framework of the network-access management solution. Putting network, application, and device management together in one integrated system does much more than offer a single pain of glass, it improves the user experience and enhances security through:

- **Customized application policies** – Once a user first connects their new device to the network, enterprise apps are distributed to the device and usage-specific policies are applied to just these apps. A data wipe only affects enterprise data, not the user's personal data.
- **Single Sign On (SSO)** – Mobile apps distributed by IT share a user's credentials so that username and password don't have to be entered each time an app is accessed.
- **Cut-and-paste restrictions** – Files connected to enterprise apps are restricted from use by a personal app.
- **Geo-tracking** – Mobile apps can be prevented from being used outside the enterprise environment.
- **On-demand VPN capability** – Mobile apps automatically establish a VPN connection so that traffic is encrypted. The user is not required to manually open the VPN.
- **Network QoS** – Latency sensitive business apps can be allocated priority over the corporate network.

By 2015, more than **50% of the worldwide workforce** will have been born after 1980. "Millennial Generation" have a longer track record and familiarity with communication, collaboration, media and digital technologies. — *Gartner adoption of mobile learning*


ARDE

ADVENTURES IN COMPLETE MOBILE ACCESS SECURITY

7 8 9

- IS THERE A SINGLE PLATFORM THAT UNDERSTANDS NETWORKING?
- WHAT ARE THE CRITERIA FOR CHOOSING THE RIGHT VENDOR FOR YOU?
- THE CRITICAL ADVANTAGE OF BEING ABLE TO SEE

IS THERE A SINGLE PLATFORM THAT UNDERSTANDS NETWORKING?

A secure BYOD deployment now means implementing a solution that goes beyond what MDM delivers today. So, let's look more closely at this BYOD approach that integrates network, application and device management in one cohesively holistic solution.

Network access management vendors actually saw this approach coming and anticipated the opportunity to control every device, including personal devices, by applying policies before and after devices connect to the network.

By centralizing policies within the purview of network access-management, BYOD rollout is simplified and new policies can be created that cross functions. For instance:

- A device that's been compromise in some way (e.g. if jailbroken) can trigger not just device specific policies but can also lock or wipe specific applications on that device and quarantine the device on the network.
- A network experiencing congestion can make changes on the devices connected to that network, such as turning off iCloud backups.
- A user moving to another location can trigger a policy that turns off a device's internal camera or another application policy, such as locking confidential applications.

These granular policies simply aren't possible if you only look at device, application and network management in silos.

How much can you empower your end users?

BYOD is also changing the end user dynamic. You want a device side mobile app that acts more like a personal BYOD portal than just a transparent management agent. You want to let a user group and manage their enterprise apps easily and also empower users to securely offload repetitive helpdesk tasks.

By empowering users to perform simple tasks directly from their devices, they can create guest credentials from anywhere.

And, registering and sharing Wi-Fi capable devices like printers, game consoles and Apple Bonjour-capable devices for data sharing is as simple as opening their secure device side mobile app.

Half of businesses state that supporting more Internet-connected smartphones and tablets is a top mobile priority.
—Forrester – Prepare for connected enterprise

WHAT ARE THE CRITERIA FOR CHOOSING THE RIGHT VENDOR FOR YOU?

Apple App store will account for **47%** of annual downloads by end of 2012 – App store added 5 billion downloads in the quarter March to June.

—Gartner Market trends Mobile App Stores

It's a formidable challenge to cut through the vendor noise and hype and identify the best third-party partner for implementing a viable, sustainable, cost-effective BYOD solution. Here are the criteria that we think are critical:

- **Experience** – For an implementation this sensitive and complex, you need a vendor with an extensive track record, particularly with clients whose specifications and legacy resources were similar to yours. BYOD really IS like brain surgery…and you don't want an intern wielding the scalpel.
- **Comprehensiveness** – Your vendor should be masters of the turnkey solution who can help you design, deploy and provide single-source maintenance of all solution components across the entire infrastructure – which is absolutely critical for providing effective policy enforcement.
- **Shortcut-savvy** – We all prefer green field projects, but some vendors see nearly every project as requiring a complete, big-budget infrastructure overhaul. On the other hand, the astute, customer-centric vendor leverages your existing infrastructure investments, and finds the appropriate integration points to provide you the best possible solution.
- **Solution-agnostic** – Big, name-brand vendors may often require you to buy into a big, name-brand – and *proprietary* – solutions. For a solution that is as cost-efficient as it is effective, find the vendor who can package a best-of-breed solution that complements and leverages your legacy resources, getting the most mileage out of both old and new infrastructure and policies.

THE CRITICAL ADVANTAGE OF BEING ABLE TO SEE

There's an old saying in network security: *You can't protect what you don't know about.* To that extent, a critical piece of the BYOD puzzle involves knowing what devices are making their way onto enterprise networks.

The challenge is that many of the devices that now connect are doing so undetected. In most cases, IT cannot distinguish between known devices that are already connected to network versus unknown devices that are new to the network.

BYOD access solutions must offer device-profiling capabilities that accurately identify a wide range of devices that request network access. Device profiling gives you the visibility to discover, categorize and maintain a database of all endpoints.

The data that is collected – MAC OUIs, DHCP fingerprinting, CDP/LLDP and device inventories – should be available for the access solution to leverage, in order to establish and enforce context-aware access policies across the entire network.

The ability to store and view information for any user or device opens up startling new management vistas, making it easier for you to plan network upgrades, adjust Wi-Fi coverage, and create reports for audit and compliance tracking.

For instance, the right BYOD solution can reveal that a specific location is inundated with BYOD connections at a specific time of day, allowing your IT staff to both respond to the real-time spike as well as do a big-picture preemptive assessment of bandwidth allocation.

Visibility also gives you better control, allowing IT to modify authorization privileges when device profile changes are detected. This means that if a printer appears as a smartphone, your access-management solution should automatically deny access and quarantines the device.

Better understanding…better control…what comprehensive visibility really gives you is a better way of doing BYOD right.

KEY TAKEAWAYS

89

> BYOD SOLVED.

> ABOUT ARUBA NETWORKS

BYOD SOLVED.

It's easy to lose sight of your top priorities when sifting through the mountains of marketing material on BYOD. Especially since the mobile universe is incredibly dynamic and continues to change every day. It's important to stay focused on the key BYOD takeaways:

- Avoid siloed BYOD point products. Insist on a fully integrated solution that handles device onboarding, network security, device and application management, and policy management from a single platform. And it should work with your existing infrastructure.
- Offload time-consuming manual tasks from IT. Instead, enable employees and guests to securely onboard their own devices and apps and manage aspects of their BYOD experience through a simple mobile app on their personal device.
- Deliver a simple and intuitive mobility experience to all users, protect company data on their mobile devices, and keep their personal information private. This will make it easier for users to adopt corporate security policies for BYOD.

The **cost of connecting personal mobile devices** to the corporate network ranges from $568 to $1,285. One-time costs start at $16, when security requirements are minimum, and can go up to $637, when a dedicated infrastructure to support a zero-footprint approach is required.
—Gartner – Cost of connecting apple's ipad

ABOUT ARUBA NETWORKS

Aruba Networks is a leading provider of next-generation network access solutions for the mobile enterprise. The company's Mobile Virtual Enterprise (MOVE) architecture unifies wired and wireless network infrastructures into one seamless access solution for corporate headquarters, mobile business professionals, remote workers and guests. This unified approach to access networks dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, Africa and Asia Pacific regions. For real-time news updates, follow Aruba on Twitter and Facebook or read our corporate blog, Aruba Atmosphere.

WANT TO KNOW MORE? CONTACT US AT:

Aruba Networks, Inc.

1344 Crossman Ave.
Sunnyvale, CA 94089
(408) 227-4500
www.arubanetworks.com

Click here for information about Aruba BYOD solutions.
Click here for information about Aruba ClearPass products for BYOD.

aruba®
NETWORKS