Conquering Today’s Bring Your Own Device Challenges
A framework for successful BYOD initiatives
Table of Contents

Introduction 3
BYOD drivers 3
  Consumer choice 3
  IT considerations 3
  Device and information overlap 4
  Application accessibility and data protection 4
  Manual and automated policies 4
  IT and helpdesk overload 5
Shortcomings of BYOD solutions 5
  Wireless, wired and multivendor considerations 5
  The point-product approach 5
  Siloed visibility 6
  Simplicity and automation 6
When BYOD works 6
  Device onboarding, provisioning and profiling 7
  Policy management based on user roles and devices 7
  Identifying and remediating compromised devices 8
  Guest Wi-Fi access 8
  Visibility and reporting 9
The Aruba ClearPass access management platform 10
  ClearPass Policy Manager 10
  ClearPass Onboard 11
  ClearPass Profile 11
  ClearPass Guest 12
  ClearPass OnGuard 12
  ClearPass QuickConnect 12
Meeting the BYOD challenge with Aruba 13
  The ClearPass advantage 13
About Aruba Networks, Inc. 14
Introduction

Today’s growing demand for anytime, anywhere network access has expanded to include the use of personal mobile devices such as laptops, tablets, smartphones, e-readers and more. This Bring Your Own Device phenomenon is changing the way IT organizations and users address network access security.

For IT organizations, BYOD means supporting a variety of devices and their operating systems, and maintaining an expected level of service. To keep costs low, it must be easy to securely onboard new devices and quickly identify and resolve problems.

For users BYOD means using the laptop or smartphone that works best for their needs. They must also understand support considerations and what happens when a device is replaced, lost or stolen.

This paper discusses the benefits and considerations associated with BYOD, and how organizations can effectively deploy a unified access management solution for any wireless, wired or VPN network.

BYOD drivers

Consumer choice

From the executive who purchased an iPhone to boost personal productivity to the college professor who redesigned the curriculum to take advantage of new tablet applications, users in all types of organizations are bringing consumer devices to work. And when they do, everyone expects access to business applications and content, not just the Internet.

As a result, the number of devices per employee is growing from a one-to-one relationship to a one-to-many relationship. A single user today will interchangeably connect to the network with a Windows laptop, and possibly an iOS or Android smartphone or a tablet throughout the day.

In fact, the adoption of smartphones, tablets and notebooks is expected to grow at a compounded annual growth rate of 25.7% through 2015.

IT considerations

In response to this consumerization of IT, organizations are not only expanding their support of Windows devices, but also embracing the demand for Mac OS X, iOS and Android devices. This often requires introducing new network components that assist in identifying these devices and enforcing network access privileges.

IT organizations will also need to consider the following when first exploring a BYOD initiative:

- Device and information overlap and security implications.
- Application accessibility per user and per device.
- Enforcement of policies.
- Automated policy enforcement.
- IT and helpdesk overload and levels of visibility.

Any Device

Galaxy Tab  MacBook  iPhone  iPad  Droid

Any Network

VPN

The Aruba BYOD Solution
Device and information overlap

Lengthy evaluations that lag the introduction of new devices are a key driver for organizations to allow users to purchase their own devices. For these reasons, some organizations are scaling back on the provisioning of corporate-owned devices and are exploring subsidized programs where the user is reimbursed for the initial purchase of a laptop as well as contributing to monthly service charges for smartphones.

The effect of granting enterprise access to personal devices does have direct implications on security, information ownership, device/network control and even helpdesk resources. These security challenges include:

- Understanding who and what is on the network.
- Keeping the network malware-free.
- Determining the level of information that can be stored on a BYOD endpoint.
- Providing proper enforcement of access policies to maintain compliance and audit requirements.

Application accessibility and data protection

As mobile devices become more mainstream, it will be difficult to differentiate access to consumer and corporate applications. FaceTime, Skype, Facebook, and others are blurring the definition of consumer applications. Collaboration applications like Dropbox and Citrix on mobile devices are driving the need to ensure that security and Wi-Fi services meet demands.

Addressing which applications can be used for personal and business applications, what can be stored on cloud services, and if virtual desktop infrastructure (VDI) applications are a requirement that must also be explored. Most organizations do not want to control what applications someone puts on their personal device, but they do want to control which applications can be used over the corporate network. In some instances, authentication of the device is a precursor to the user then initiating a Citrix session to ensure access to confidential data.

As this use your own application on BYOD devices proliferates, organizations must consider a network policy management system that addresses the concerns below and interoperates with external mobile device management applications that monitor device usage:

- Instant messaging
- Video and photography storage
- E-mail and texting
- Internet browsing on and off campus
- Device tracking
- Wiping of devices or containers

Manual and automated policies

The adoption of BYOD requires each user to understand the implications of personal devices, the type of information that can be stored on these devices, and what is expected of them to meet pre- and post-authentication requirements.

While manually distributed policies are a start, automated policy enforcement lets organizations leverage information from the devices themselves. This promotes a policy enforcement approach that's based on real-time changes in device risk, physical security and time of day.

For example, depending on the device, ensuring that access to corporate information and the use of anti-virus and peer-to-peer applications are met before and during a network access session becomes a process that can actually be maintained without much interaction by the user or IT.
IT and helpdesk overload

Similarly, IT and helpdesk resources can be quickly overwhelmed as the organization struggles to configure and support these new BYOD endpoints for secure network authentication and corporate use. Automated tools that allow end-users to securely self-onboard their devices are critical to offload the helpdesk organization.

The visibility needed to support successful and unsuccessful authentications will also increase as new devices are introduced and users adopt new applications that meet or might not meet corporate guidelines. The ability to quickly find entries corresponding to individual users and information on specific devices is essential – regardless of how or where users connect.

Shortcomings of BYOD solutions

Wireless, wired and multivendor considerations

Numerous network access products are available today, many of which are being positioned as BYOD solutions. However, most fall short of providing the necessary scope required to span wired, wireless, and VPN infrastructures and to support employees, contractors and guests and the myriad devices they own.

Solutions from infrastructure vendors, for example, ignore the multivendor nature of most enterprise networks, leaving gaps in coverage that may require additional point solutions. Some solutions only focus on Wi-Fi while others require a client on the end-device that only works with mobile operating systems like iOS and Android.

<table>
<thead>
<tr>
<th>Wired Switches</th>
<th>Wireless APs</th>
<th>VPN</th>
<th>Managed Endpoints</th>
<th>UnManaged Endpoints</th>
<th>Endpoint Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aruba</td>
<td>Aruba</td>
<td>Aruba</td>
<td>Windows</td>
<td>iPhone/iPad</td>
<td>NAP, NAC</td>
</tr>
<tr>
<td>Cisco</td>
<td>Meru</td>
<td>Cisco</td>
<td>Mac</td>
<td>Android</td>
<td>A/V, A/S</td>
</tr>
<tr>
<td>HP</td>
<td>Meraki</td>
<td>Juniper</td>
<td>Linux</td>
<td>Printers</td>
<td>Firewall</td>
</tr>
<tr>
<td>Enterasys</td>
<td>Cisco</td>
<td>SonicWall</td>
<td>F5</td>
<td>VoIP Phones</td>
<td>Discovery</td>
</tr>
<tr>
<td>Extreme</td>
<td>Motorola</td>
<td>Check Point</td>
<td>and More</td>
<td>Medical Devices</td>
<td>Patch Management</td>
</tr>
<tr>
<td>Juniper</td>
<td>Xirrus</td>
<td>and More</td>
<td></td>
<td>MFG. Devices</td>
<td>Vulnerability &amp;</td>
</tr>
<tr>
<td>Foundry (Brocade)</td>
<td>and More</td>
<td></td>
<td></td>
<td>Security</td>
<td>Port Scans</td>
</tr>
<tr>
<td>and More</td>
<td></td>
<td></td>
<td></td>
<td>Equipment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(cameras, etc.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>NAP, NAC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>A/V, A/S</td>
<td></td>
</tr>
</tbody>
</table>

Adaptable to any customer infrastructure

The point-product approach

A number of BYOD security solutions are merely point products that offer one solution for laptops, one for mobile devices, and so on. This approach to network access policy management and BYOD is complex and costly to implement, requiring IT to purchase and support multiple components that do not interoperate well with the existing network infrastructure.

Such complexity can also be an impediment to users by requiring manual device provisioning, which results in a flurry of helpdesk calls. Device provisioning must be simple for users in order to discourage them from attempting to circumvent it.

Users need the flexibility to securely self-provision a device or utilize a sponsor role within the guest access process, regardless of access method. This makes it easy for any user to onboard with little or no IT intervention.
IT organizations need the flexibility to define policies based on multiple variables, including:

- When and where a given type of device, such as a smartphone, can be used.
- What resources that specific user is allowed to access via that device.
- What services and applications the user can run from that device.
- How much bandwidth a given device or application is allowed to consume.

**Siloed visibility**

IT needs a solution that provides complete visibility into what IT-managed and BYOD devices are admitted onto the network. Real-time visibility, including device profiling, is a prerequisite for granular access control as well as for reporting, planning, auditing and compliance.

For example, only with these tools in place can IT verify that the chief financial officer’s lost smartphone hasn’t been used to gain access to sensitive data. A siloed model often requires the IT to monitor multiple tools, which is counterproductive.

**Simplicity and automation**

Solutions that lack basic onboarding and per-session data force organizations to spend less time on business-critical projects and more time performing manual troubleshooting and diagnostics.

While it may seem daunting to support BYOD, organizations can embrace this trend by taking a holistic approach that automates processes and takes into consideration IT and user requirements as well as work habits.

**When BYOD works**

Organizations can reap a wide range of benefits by embracing BYOD initiatives, including the ability to quickly support user needs and devices, boost productivity, and in many cases, reduce expenses.

One of the first things to consider when deploying secure BYOD is a simplified workflow that can accommodate all device types, work with the existing infrastructure, and allows organizations to start small, measure progress and then easily support additional requirements on the base platform as needed.

**BYOD access deployment strategy**

- **Prohibit**
  - Only allow corporate specific devices
  - IT designated devices
  - IT managed devices
- **Limit**
  - Internet and select resources
  - Select BYOD devices
  - User managed devices
- **Trust**
  - Full access
  - Differentiated BYOD devices
  - IT provisioned, user managed devices
- **Embrace**
  - Any device, any location access
  - Multiple differentiated BYOD devices per user
  - IT and user provisioned

**Implement and Adjust**
To address these challenges, Aruba Networks® developed the ClearPass Access Management System™. A key part of the Aruba Mobile Virtual Enterprise (MOVE) architecture, ClearPass provides a user- and device-independent framework that tackles any BYOD initiative, large or small, by providing:

- Self-service onboarding, provisioning and revocation of access for all major mobile devices.
- Device identification as a basis for grooming traffic and improving network security.
- Consistent policy enforcement across multivendor wireless, wired and VPNs.
- Controlled access and remediation for compromised devices.
- Secure guest network access with simplified workflows.
- Enhanced security, reporting and regulatory compliance.

**Device onboarding, provisioning and profiling**

A BYOD solution must automate the authentication and device onboarding process so that employees, contractors, students and guests can self-register devices for secure access to secure wireless and wired networks, as well as VPNs.

Supported device types:

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Wi-Fi Access</th>
<th>Wired Access</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Windows 7, Vista, XP</td>
</tr>
<tr>
<td>iOS</td>
<td>Yes</td>
<td>N/A</td>
<td>4.x and up</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>Yes</td>
<td>Yes</td>
<td>10.5 and up</td>
</tr>
<tr>
<td>Android</td>
<td>Yes</td>
<td>N/A</td>
<td>2.1 and up</td>
</tr>
</tbody>
</table>

Underlying complexity must also be removed to easily configure network and posture assessment settings, and provision and revoke certificates or unique device credentials to ensure that only approved devices are used.

User and device information captured during self-registration and device profiling will allow organizations to create and manage policies that are far more granular than those where only baseline fingerprinting or using MAC address authentication is performed.

Profiling should include baseline dynamic host-configuration protocol (DHCP) fingerprinting and browser detection, as well as collecting detailed information from sources such as agents, RADIUS authentication servers, and Active Directory data.

**Policy management based on user roles and devices**

The administration and enforcement of policies based on user role and device type lets organizations create and enforce policies that apply to a group of users or devices. It also leverages other contextual information that pertains to either the user or device within policy enforcement.

For example, organizations can ensure that access to appropriate data is different for the engineering staff versus the finance staff to satisfy internal and external compliance mandates. Additional contextual data on device roles ensure that access for known laptops is different from iPads that have Internet-only access through a BYOD program.

No two organizations are exactly alike, so BYOD has different connotations depending on who you talk to. To some users, like a doctor, it means bringing a laptop or tablet to work and accessing electronic medical records (EMR). To a college professor, it may mean hosting a conference, easily acquiring guest access for each user and ensuring secure access regardless of the type of device.
An effective BYOD access management solution must be vendor neutral, based on open standards, and leverage an enterprise's existing security, identity and network infrastructure. Policy enforcement methods must have the flexibility to satisfy the majority of use cases that organizations want to support, such as role-based policy management, VLAN steering and SNMP enforcement for captive portals.

In the aforementioned examples, policies can be enforced across any network – wireless, wired and VPN. Identity stores, user-roles, and authentication methods are updated as the policy system receives real-time profiling and visibility information.

Identifying and remediating compromised devices

A BYOD access solution should provide enterprise-class posture assessment and remediation that's a cut above ordinary network access control (NAC) offerings. It must go well beyond traditional health checks to also examine a device’s runtime configuration and applications, and whether USB storage devices are allowed.

The ability to use permanent and dissolvable agents is important as many of these devices will be administratively managed by the user. Dissolvable agents for BYOD reduce administrative overhead as they are downloaded during a captive portal login and removed once the web page is closed.

In addition, enterprise-class posture assessment solutions typically compare the posture/health information against policies defined in a centralized policy decision point (PDP). For a BYOD access management solution to be effective, the PDP must have the ability to automatically quarantine non-compliant BYOD and IT-issued devices using role-based mechanisms or VLAN steering methods.

As part of a comprehensive posture assessment approach, a BYOD access solution should:

- Perform automated checks via persistent and dissolvable agents.
- Check for up-to-date antivirus, antispyware and firewall software.
- Check for USB storage and peer-to-peer applications and services, such as Skype and BitTorrent.
- Provide control options, including protected network access, manual and auto-remediation via directed URLs, and denial of service.

Finally, tying posture information with identity-related and other contextual data allows organizations to enforce differentiated policies as business needs dictate.

Guest Wi-Fi access

The definition of a guest user is much more complex now and could mean anything from a temporary contract employee to a shopper in a retail environment. As a result, a BYOD access management solution must provide similar capabilities for guests as well as for employees – including dynamic provisioning, profiling and role differentiation – which are needed to ensure that compliance requirements are met.

Many organizations restrict guests to an isolated network segment, such as using a separate SSID from the corporate SSID, and provide Internet access only. However, the BYOD access solution should give IT the flexibility to create different access rules for different types of visitors.

In addition, a guest solution must be easy to use, support multi-tiered administration and sponsor capabilities, and automate the ability to include contextual elements within policies that take into account time-of-day and day-of-week privileges.

For example, when a guest enters information requesting access, the BYOD access solution must have the ability to create an account that sits in a disabled state until an approved sponsor has verified and approved the request. Automated methods must exist that deliver access credentials over SMS or email once approval has been received by the system.
Visibility and reporting

To address compliance and regulatory requirements, collection of transactional data for each user session offers IT and business managers a variety of deployment, troubleshooting, and reporting options.

**Web-based management.** Providing IT staff with web-based access to the entire policy management system without requiring dedicated appliances or licenses ensures ease of use and a lower total cost of ownership.

**Centralized policy management.** In large deployments, IT needs management capabilities from a central location to ensure that policies are effectively deployed and managed to adhere to organization and user needs. For example, IT staff in Los Angeles should be able to define policies for remote workers in India or China. The time and cost savings are easily recognized – resources and travel budgets are not required to support new users and use cases or to perform troubleshooting.

**Multiple administration levels and role-based access.** While policy management must be centralized to ensure consistency, organizations need the flexibility to administer policy management in a distributed fashion. A BYOD access solution must support a range of administration levels and role-based administration across the security, IT and helpdesk organizations.

**Access analytics and reporting.** Visibility into access activity is crucial to meet compliance requirements and enhance the effectiveness of network access policies. A BYOD access solution must provide IT with advanced reporting capabilities that monitor current and archived access activity, generate a variety of reports, and analyze data based on access parameters by role, class of device and access location.

IT also needs the ability to aggregate data, as well as apply filters and drill down for in-depth views.
The Aruba ClearPass access management platform

Aruba understands the challenges that organizations face when implementing an access solution that is robust yet flexible enough to handle the burgeoning BYOD trend. Aruba ClearPass is the only standards-based BYOD solution that provides access control as a non-disruptive overlay to an organization’s existing network.

As a result, an organization can leverage its existing network, identity and security infrastructure and simply turn on ClearPass functionality as needed. It’s a very cost-effective and adaptable approach that enables organizations to implement a BYOD solution that’s tailored to their particular needs.

The ClearPass Access Management System includes the ClearPass Policy Manager appliance and the following feature-rich software modules:

- ClearPass Onboard
- ClearPass Profile
- ClearPass Guest
- ClearPass OnGuard

A separate cloud-based application, ClearPass QuickConnect, makes it easy for users to self-configure 802.1X settings on their Windows, Mac OS X, iOS, Android and Linux devices for network authentication and connectivity.

ClearPass Policy Manager

The ClearPass Policy Manager combines all the capabilities of a robust BYOD solution on one platform. This central policy server provides differentiated, context-based access control, along with operational utilities designed to reduce IT overhead.
With ClearPass Policy Manager, IT can easily automate and extend authentication and authorization policies across the entire organization for wireless, wired, VPN and guest access applications. Differentiated access capabilities based on a variety of attributes, including user role, device, time, and location are also available.

In addition to its integrated policy management engine, RADIUS and TACACS+ servers for AAA support, the ClearPass Policy Manager can read from multiple identity stores and databases, including those based on Microsoft Active Directory, LDAP, SQL and Kerberos. This provides a unified policy model that ensures access controls are applied consistently across the organization.

Hardware and virtual machine (VM) options provide organizations flexibility in the form factor they choose and the ability to mix and match hardware-based appliances and VM implementations with no discrepancy in features or functionality.

Using VMs, for example, can reduce cost and complexity by lowering power and cooling requirements and simplifying cabling. Similarly, hardware appliances may be the best choice in larger data centers, while the VM option can be added to a server in remote offices when cost is a concern.

Redundancy and failover is mandatory for an enterprise-wide policy server. Rather than dedicating a fully redundant appliance to passive/standby in an active/passive model, the ideal access management solution should support fault tolerance using a publisher-subscriber model. In this model, a primary server replicates or publishes all changes to one or more secondary servers. This approach is more flexible than other clustering models.

**ClearPass Onboard**

ClearPass Onboard, the enterprise provisioning software module for ClearPass Policy Manager, fully automates device onboarding for IT via a built-in administration interface. It offers full self-service provisioning for Windows, Mac OS X, iOS, and Android devices, and includes the configuration of 802.1X settings as well as the distribution and revocation of unique device credentials.

Additional features include the ability to push configuration settings for mobile email with Exchange ActiveSync and VPN clients for some device types.

**ClearPass Profile**

ClearPass Profile, the device profiling software module for ClearPass Policy Manager, uses a five-tier system that includes DHCP and other advanced methods as well as end-user and device fingerprinting and profile information. Device-level information includes details such as operating system version, manufacturer and device category.

This contextual information is stored and used to enhance policy decisions and to identify changes in a device’s profile, which in turn dynamically changes authorization privileges. For example, policies can be used to differentiate access for an employee’s company-issued device versus the same employee’s personally-owned device.
Conquering Today’s Bring Your Own Device Challenges

ClearPass Guest

The ClearPass Guest software module for ClearPass Policy Manager enables IT as well as non-technical personnel to manage guest Wi-Fi accounts and onboarding tasks when providing network access for visitors in large and small environments.

In addition to allowing employees and guests to self-register their own devices, ClearPass Guest supports role-based access controls, activity tracking for compliance and auditing, and unique features such as advertising and commercial-grade hotspot services.

ClearPass OnGuard

The ClearPass OnGuard software module for ClearPass Policy Manager enables comprehensive posture assessments that minimize the risk of viruses and the misuse of applications and services before devices connect to the network.

Supporting persistent and dissolvable agents, including vendor-specific agents such as Microsoft Windows native supplicants, ClearPass OnGuard performs posture assessments on devices running Windows, Mac OS X and Linux operating systems, checking for the presence of anti-virus, anti-spyware, and firewall software from more than 80 vendors.

ClearPass QuickConnect

ClearPass QuickConnect is a cloud-based service that provides simple self-service 802.1X configuration for Windows, Mac OS X, iOS and Android devices, reducing the overhead burden on IT.

IT configures endpoint variables to create network authentication packages, while users are presented with a configuration wizard via a captive web portal, Active Directory group policy object (GPO), USB device or CD. Users simply start the wizard, enter their credentials and connect to the network in minutes.

Automated posture and health remediation
Meeting the BYOD challenge with Aruba

As BYOD initiatives proliferate, organizations are under pressure to simplify the process of connecting new users and devices while maintaining strong security and keeping costs down.

The Aruba ClearPass Access Management System is the industry’s first BYOD platform that takes a holistic approach to securing the mobile user, devices and network infrastructure. ClearPass provides a comprehensive standards-based, vendor-neutral solution that enforces access policies across any network, any device and any user.

The ClearPass advantage

Aruba ClearPass provides a simple, cost-effective and multivendor approach to connecting and securing BYOD and IT-managed users and devices.

ClearPass delivers the following advantages for successful BYOD today:

- User and device self-registration and onboarding to reduce the burden on IT.
- Ability to deploy with Aruba access networks or existing infrastructure.
- Unified visibility and control from a single platform.
- The industry’s most intuitive administrative interface.
- Centralized policy management and enforcement.
- A consistent user experience regardless of device or location.

For further information and assistance regarding BYOD best practices, contact Aruba Networks to discuss your BYOD lifecycle plan.
About Aruba Networks, Inc.

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, and Asia Pacific regions. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook.