EXECUTIVE BRIEF

DESIGN SECURITY POLICIES FOR #GENMOBILE

Look around the office and you can't help but notice that everyone's using mobile devices and nobody's at their desk. Mobility is the essence of this next-generation workforce, #GenMobile. Mobility—and the newfound flexible work style that it's unleashed—create a challenge for IT to provide users with secure, dependable access to applications, printers and other network services, regardless of their device or location.

IT must ensure that the wired and wireless infrastructure for #GenMobile provides a personalized mobility experience that everyone can rely on and trust. But this doesn't have to be a formidable task. It's possible to go well beyond mere authentication and give users secure access to apps, printers and other network services from both IT-managed and personal devices if you focus on four key areas.

Match roles to resources: The days of giving users access to static set of internal applications and web-based resources is long gone. Authentication-based access control was fine when each user had one wired device in one desktop location. But the growing number of mobile users on today's wireless networks requires access privileges based on contextual information that includes user role, types of devices in use and location.

Automate device onboarding: When employees bring their own devices to work, someone in IT has to manually configure security settings and issue certificates for these hundreds, sometimes thousands, of smartphones and tablets. It's an endless, time-consuming chore, made worse when devices are lost or stolen or users want to onboard new devices. IT needs tools that automate onboarding of new devices with security, network and app configuration.

Go beyond Mobile Device Management (MDM): MDM is great for denying the use of certain apps, detecting a device's location and performing a data wipe – when devices don't have a Wi-Fi connection. But MDM can't stop jailbroken devices from connecting to the enterprise Wi-Fi network, nor does MDM prevent the use of blacklisted apps. You need stronger device security for that.

Deliver secure guest access without IT assistance: Wide-open guest access—that is, handing out shared credentials and finding the one person in IT who can give a visitor network access—isn't working. This approach is inherently insecure, is easily abused, and is an incredibly inefficient use of IT resources. You need a Wi-Fi solution that maximizes security for guest access while minimizing IT involvement.

ESSENTIAL SECURITY TOOLS FOR #GENMOBILE

Aruba Networks deliver security features designed for #GenMobile. With built-in policy and AAA services, the Aruba ClearPass Access Management System™ makes it amazingly easy to create and enforce policies based on a user's role, device type and location. IT can now automatically differentiate which resources a personal device can access versus IT-managed devices.

ClearPass leverages the role-based policies you already created to automate device onboarding, so employees can on-board their own devices without IT involvement. Its built-in certificate authority automatically issues unique device credentials to everyone, which simplifies authentication and makes it easier to revoke certificates for lost or stolen devices.

ClearPass also ensures that wireless policies integrate with MDM servers to secure the network when users connect personal devices. That means devices can't connect if they're jailbroken or missing the MDM agent. ClearPass can also trigger your MDM system to automatically generate a helpdesk ticket and device notification when users are prevented from connecting.

In addition, Aruba ClearPass makes it possible to secure guest access without IT assistance. ClearPass Guest lets IT control who gets network access and issues unique guest credentials that separate guest traffic from enterprise traffic - with no IT involvement. Guest-specific role enforcement automatically assigns where, when and how long a guest can stay on the network. Once guests have logged into a captive portal, a MAC caching feature remembers their credentials so guests don't have to keep logging in throughout the day.

SUMMARY

It's possible—even easy—for IT to go beyond authentication and protect enterprise data while giving #GenMobile an all-wireless workplace. The best way to get there is by matching roles to resources, automating device on-boarding, integrating with MDM, and simplifying guest access. With the right security approach, enterprises can give #GenMobile secure access to apps, printers and other network services, no matter where they are or what device they use.

To learn more, visit **www.arubanetworks.com/allwireless/** or contact Aruba Networks at **info@arubanetworks.com;** +1 866 55 ARUBA (+1 866 552 7822).

aruba NETWORKS

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com