EXECUTIVE BRIEF

ENABLING SECURE ENTERPRISE MOBILITY

Why smart devices require a different approach to security

If you're like most, sitting at a desk for the entire day and only carrying a laptop is a thing of the past. Life was simple and you could always reach email, apps and the printers needed. The new generation of worker, known as #GenMobile, uses multiple mobile devices for every aspect of work and personal communication and stays connected, no matter where they are.

Fortunately, implementing secure enterprise mobility for #GenMobile doesn't have to be complex or involve a full-scale overhaul. By focusing on four simple things, you can have stronger security, improve the app and device experience for everyone, and reduce IT helpdesk calls.

- Enhanced visibility
- Contextual policies
- Workflow enablement
- Role-based enforcement

ENHANCED VISIBILITY

If you can see it, you can use it

Work information on potentially thousands of employee's personal devices greatly increases your exposure to vulnerabilities. That's why it's important to know who and what's on your network. The days of tracking devices with a manual database or asking users to fill-out complex registration forms is not the answer.

Dynamically profiling devices as they connect is the best option. It gives IT valuable information that can be used for policies and troubleshooting. Policies that use real-time data make it easier to allow or restrict access to resources based on users, device types and assumed risk levels.

CONTEXTUAL POLICIES

Policies that stick no matter what

Although legacy authentication, authorization and accounting (AAA) can enforce basic network privileges, it offers little flexibility. Policies that use contextual data like location or time of day are more effective in the mobile enterprise. In fact, 70% of #GenMobile prefer flexible hours versus working 9 to 5.

Differentiating how a user or device authenticates is also important from a security standpoint. Logins and passwords are being replaced with certificates as smartphones and tablets gain in popularity.

In addition to being more convenient for users, this approach lets IT circumvent brute force password attacks and eliminate calls due to locked out devices whose passwords are out of sync in Active Directory.

WORKFLOW ENABLEMENT

Put device configuration on autopilot

To handle rapidly growing mobility and BYOD initiatives, automatic provisioning lets users self-configure their devices for enterprise use. If a new device tries to connect to the network, relevant settings and a unique certificate are automatically placed on the device without IT assistance.

It's a good idea to move certificate distribution and revocation services from your mobile device management (MDM) system to an access management platform. You'll be able to include unique user and device attributes in a certificate and prevent exposing an internal PKI for IT-managed devices to a host of personal devices.

CONTEXTUAL POLICY ENFORCEMENT

Trust and security using everything you've learned

Mobility has completely trivialized the idea of creating separate VLANs for everything – user groups, workspaces and traffic types – to enforce network privileges. As Wi-Fi becomes the dominant way to connect, users can do it from anywhere and use voice, video and data apps from the same device.

Another big advantage of mobility is you no longer have to configure VLANs over and over again. Take everything you know about creating policies, apply it to your infrastructure using contextual data, and users will be automatically directed to appropriate resources without the IT burden.

SUMMARY

Secure enterprise mobility for #GenMobile isn't difficult, but it does require some critical thinking about policies and enforcement. A flexible and comprehensive access management platform ensures that security and compliance requirements are met without sacrificing the user experience or over-burdening IT.

For more information, please refer to the ClearPass Solution Overview or contact an Aruba representative at info@arubanetworks.com.

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