aruba
a Hewlett Packard Enterprise company

EXECUTIVE OVERVIEW

BYOD DOESN'T HAVE TO BE YOUR BIGGEST HEADACHE

8 Best Practices to Protect your Enterprise Network

Smartphones and other personal devices can now be found in most businesses as users are staying connected to the corporate network from anywhere, any time. It's the stuff that keeps IT and security managers up at night — mobile users, multiple devices per user, and enterprise data on the move.

Security for Bring Your Own Device (BYOD) and mobile must now be part of a larger conversation when securing the network for the new digital workplace. Based on existing customers' best practices, this paper outlines eight things you can do to boost network security amidst BYOD.

1. ASSIGN ROLES TO USERS AND DEVICES

With users carrying multiple devices, it's smart to standardize on user roles across the organization, and then assign device roles, too. A smartphone issued by IT for a specific purpose may require more access privileges than a personal device. IT-issued laptops would have different roles than smartphones and tablets. The value is your ability to create different rules for each device type or role.

User and device roles also let you differentiate privileges by device type for the same user. An IT administrator would be allowed to change switch and controller configurations with a laptop assigned a corporate role. But, that same person would not be able to access sensitive networking equipment using a tablet assigned a BYOD role.

2. USE PROFILING TO CREATE DEVICE CATEGORIES

Accurately profiled devices should be a cornerstone of your plan when rolling out a secure BYOD initiative. As BYOD permeates throughout your environment, not all users will be diligent about downloading the latest versions of the operating system. You'll want to capture context that allows you to see who is running what versions on iOS, Android, Chrome and other operating systems.

As new releases become available, this data will give you the visibility to help identify why authentications may be failing, the types of devices that are experiencing issues, and more.

IT has to support any device that users choose.

An understanding of location can also help determine if a problem is specific to Wi-Fi equipment if the enterprise is operating a multivendor environment.

3. USE CONTEXT WITHIN POLICIES

It's important to leverage multiple sources of context to manage access. Data can consist of user role, device profiling, location, and once a certificate is issued to a specific user's device, the assumption is that it's a BYOD. Doing this greatly enhances productivity, usability and security. By enabling the use of known data you can stop users from coming up with ways to bypass policies.

The use of device categories should also be explored. The idea is to again leverage context to enforce privileges across a large category of devices. All BYOD endpoints connecting over a VPN can be treated differently than when connecting in the office. Printers can be managed differently than game consoles or Apple TVs.

4. MANAGE MOBILE APP USE

Today, 70% of connected devices within an enterprise can be categorized as BYOD. IT must now consider controlling the apps used on any given device when it's connected to the network, which is not as easy as it sounds. While corporate EMM containers and MDM application "stores" can help limit application downloads, Google and Apple App stores do not. Your employees will most likely install any app they want.

Enterprises need to define and enforce policies that dictate who can access specific types of data from which devices, with the ability to differentiate between smartphones, tablets, laptops or IoT devices. To be effective, enforcement must extend across MDM/EMM, a policy management platform, and firewalls.

5. AUTOMATE AND SIMPLIFY

Automation is essential for both initial onboarding and to take action on non-compliant devices (for example, quarantining them until they are compliant). MDM/EMM solutions should share device posture with a NAC solution to ensure that devices meet compliance before being given access. Integrating with helpdesk applications and SIEM can provide an enhanced experience for the user and IT for improved problem resolution.

By automating the discovery and onboarding of non-compliant devices, you can reduce costs and improve your security posture. This also allows users to re-onboard their own devices when smartphones and tablets are replaced, which also reduces the time IT has to spend on device onboarding.

6. GO WITH CERTIFICATES – THEY'RE MORE SECURE THAN PASSWORDS

Users will connect to guest networks more frequently leaving passwords exposed to theft, which makes certificates a cornerstone of a secure mobile device deployment. As the use of active directory and an internal PKI for BYOD is not a best practice, an independent Certificate Authority (CA) built to support personal devices is preferred.

A policy management solution that includes the ability to distribute and update, as well as revoke certificates should be explored. Integration with an MDM/EMM solution should be an option in the event that device management was deployed prior to investing in a network access policy management solution.

7. MAKE EVERYONE HAPPY – SIMPLIFY SSIDS

Multiple SSIDs complicate life for IT and users alike. With effective policy management enforcement in place, BYOD and corporate-owned devices can connect to common SSIDs. Reducing the options for users to choose from simplifies the user experience, and makes it easier for IT to maintain SSIDs across multiple locations. Consolidation of SSIDs can also improve Wi-Fi performance.

The key to improving your security posture revolves around your ability to leverage roles, location and policy enforcement to ensure that devices receive the access that IT expects, even when using common SSIDs. When personal devices are connected to a common 802.1X network, IT can provide Internet access only if desired.

8. CONSIDER NEXT-GENERATION MULTI-FACTOR AUTHENTICATION (MFA)

These days, enterprise data access is often initiated from smartphones and tablets. As these devices are easily shared, many IT professionals are turning to new forms of MFA to ensure that the user of a device is really the person requesting access. Instead of token generation devices that are easily lost, there's a better way.

Now when a user connects to a network or opens an application, IT can require a secondary challenge that is as simple as picking up your smartphone and scanning your fingerprint, taking a selfie, or clicking on a pre-determined image from within the images library.

CONCLUSION

The continued rise of BYOD is inevitable, and few corporate leaders will pass up the productivity gains of a mobile workforce that pays for their own devices. But it is easy to lose track of long-term goals if you don't have a solid plan. The eight ideas presented in this paper are just some of the things that IT should consider when preparing for BYOD.

In the end, a central component that brings everything together starts with an advanced policy management platform. One that includes AAA services, NAC, BYOD onboarding and third-party integration with event-driven remediation.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com