aruba
a Hewlett Packard Enterprise company

DEFINITIVE GUIDE:

Securing the Mobile Enterprise

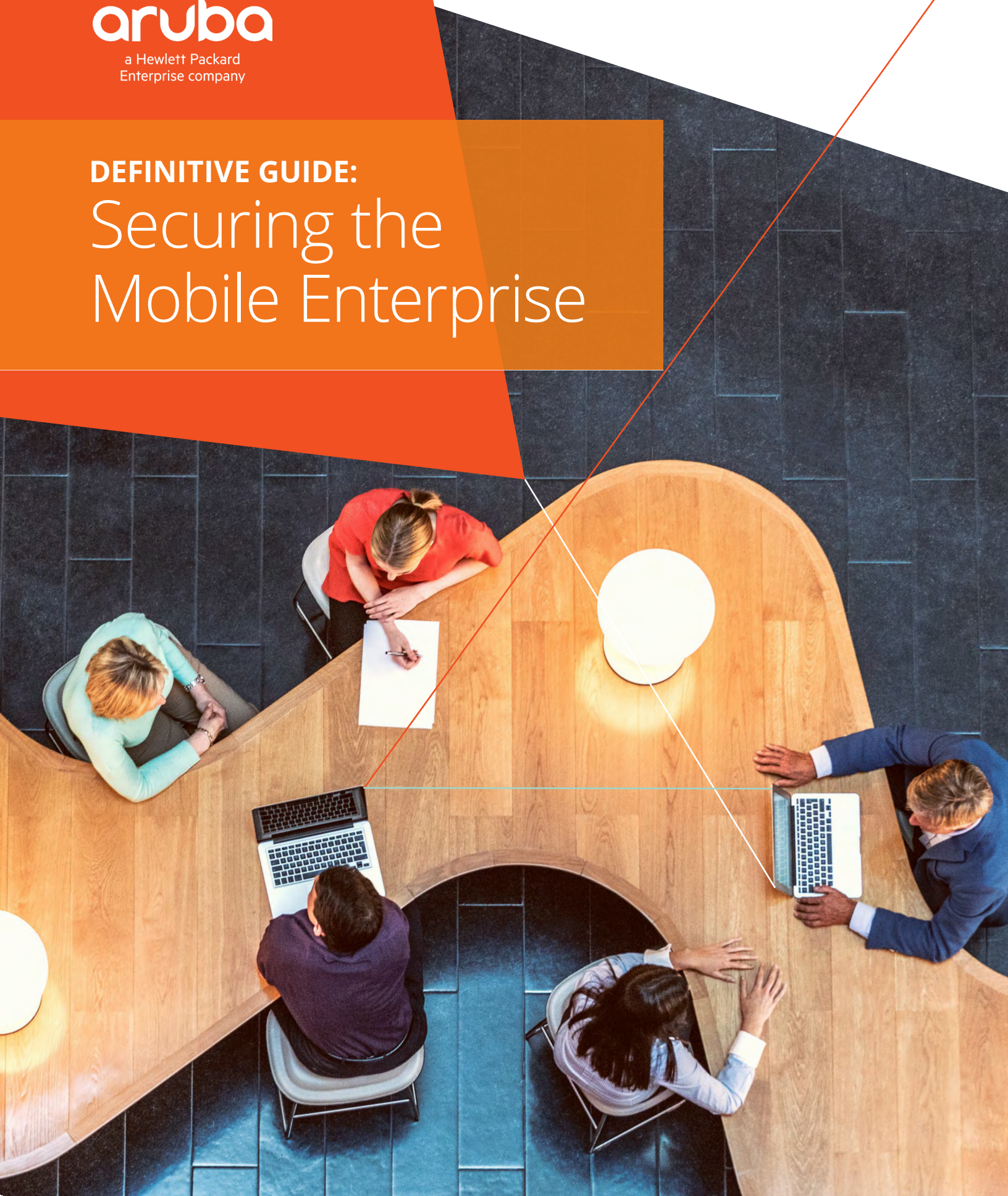

TABLE OF CONTENTS

A mobile workforce can be productive anywhere.

Executive Overview

While mobility and Internet of Things (IoT) offer potential rewards for organizations — a mobile workforce that can be productive anywhere, the promise of smart spaces — the thought of all of those unknown devices connecting to the network is the stuff that keeps security and IT managers up at night. The goal of this paper is to outline the pre-planning and deployment steps needed to help guide you on your journey of enterprise BYOD and IoT.

We'll cover how policies can help control BYOD and poor user behavior, regardless of whether your road. We'll also highlight how profiling and context can create an environment that allows for differentiated access based on user roles, device types, ownership, and location.

Lastly, we'll discuss how greater visibility and the integration of your policy decision engine with third-party security solutions can enhance your ability to offer end-to-end mobile protection — from device, access layer, and traffic inspection to security information and event management.

SECTION 1: The Basics

Acknowledging User Behavior and Trust

Today's #GenMobile workforce has completely diluted the notion of a fixed perimeter – it doesn't exist where users connect and work from anywhere. Added pressure comes from users expecting the same access privileges regardless of device or location. And, as no two users are identical, this creates an interesting challenge for IT organizations.

Some users will primarily work from the office, while others may call the road their workplace. A large majority will enable pin codes on mobile devices and adhere to the use of VPNs while outside of the office, but then there are those that won't.

To protect the enterprise and resources, IT must consider security that starts from inside the enterprise, but extends outside. Policies must map to individuals or groups that share similar roles and business objectives. We call this approach **Adaptive Trust Defense**.

Beyond Zero Trust

In the past, IT would treat all users with a zero-trust mentality as most users carried a single IT-managed device that was plugged into a locked-down wired port. But, today's users carry up to four devices and primarily connect via wireless.

Bring your own device (BYOD) and cloud services have also changed how, when, and where enterprise apps and data are being accessed. As all users are not equal, care must be taken to provide proper access privileges based on multiple attributes, like role, device or location.

While all sales executives may require access to sales data, not all need to see HR information for every sales manager. Within engineering, not everyone will be working on the same projects or hold the same employment status. Policies must leverage usable context.

Even perimeter security must be mobile.

Perimeter Security As We Knew It

In the past, once someone determined that your corporate assets were of value, breaching exterior walls was an easy way to gather and take what they wanted. The bigger issue today stems from internal assets that are loaded on smart devices and carried out the front door.

In fact, consumer apps are now downloaded on those same devices and carried into the enterprise, causing reverse concerns. Do the apps contain malware? Can all consumer apps be blacklisted? And how can IT keep up?

The days of solely using perimeter firewalls to keep out the bad guys is long gone. Vendors in the space are responding by integrating security apps and other tools for application-level security that begins with the device, the connection, and the traffic that originates from these devices. Even perimeter security must be mobile.

SECTION 2:

Leveraging Usable Data

Context as a Starting Point

Users can easily change the status of their mobile devices, so it is now more important than ever to archive context that starts with the device. If you can determine whether a device is jailbroken, you can solve network problems early.

The next step is to associate users with their devices to better understand where differentiated policies can be leveraged. A two-step process that leverages device attributes pulled from an EMM/MDM solution, combined with data from a policy solution can provide more granular visibility and enforcement.

The third component would be to then share usable context with security components outside of the login process. If a firewall can differentiate between a smart phone and laptop for the same user, this allows for application level policies and accurate enforcement.

It Takes a Village

In the past, security solutions like policy management, next-gen firewalls, VPN gateways, and profilers were deployed to solve specific needs. While each of these solutions are still needed, they used to lack a cohesive way to protect enterprise resources. For instance, personal devices that download freely from an app store open up a number of new threats – from inside and outside the perimeter.

Today's mobility dictates that mobile security solutions share context and enforcement actions to actively monitor and enforce access privileges. A firewall event should be able to trigger a policy change without human interaction.

"By 2018, 66% of networks will have an IoT security breach."

- IDC

1.3B+
mobile workers and growing

2/3
are NOT office based

67%
use BYOD regardless of office policy

A Common Data Exchange Model

In the old days, before modern communication, drums were a common method for exchanging information. While this worked to communicate from village to village, people were limited to a local language and range. This lack of a common language is the core issue with solutions that different vendors offer today. The digital age requires a model where data can be exchanged across multivendor platforms and remote locations.

If a user in a remote location tries to access the network, policy dictates that user and device context must be shared between security solutions, via standards-based API and syslog messaging.

A firewall can accurately enforce a policy based on a user and a specific device. A policy management solution can leverage MDM context to keep jailbroken devices from accessing confidential data. The goal is to extend this capability to a variety of vendor's solutions, so that customers have a choice.

SECTION 3:

Per User Security

ClearPass Exchange integrates contextual data with third-party IT systems for end-to-end policy enforcement and visibility.

The Platform - Aruba ClearPass and ClearPass Exchange

Similar to village dynamics, a central context collection point ensures that conditions and updates are easily accessible and shared with those requiring status updates. This is the role of Aruba ClearPass Policy Management Platform as it is the center of all authentication and authorization.

ClearPass also leverages real-time, contextual data from a variety of trusted components – MDM/EMM, identity stores (AD, LDAP, etc.), certificate authorities, and access and security components – Wi-Fi, wired, SIEM, and firewalls. Built-in REST-based API and Syslog messaging within ClearPass Exchange provides the common exchange model.

IT can automate policy enforcement when a user/device joins a network, as well as their behavior once the device is connected. For example, if a user's role is within human resources, access privileges would map to their job. Once connected, if the device does not meet a firewall policy, access to specific applications can be denied.

Knowing Your User Community

Just like a census helps determine if services meet the demographics of a city, the same principle holds true for mobility. But, unlike census polls, you can't wait years to understand who is connecting to your network and with what devices.

Using identity stores, profiling and onboarding tools to better define policies is a must. Pulling user data from an active directory (AD) helps determine employees from guests. In fact, the AD attributes can even help keep employees from using a guest network during business hours. Profiling and onboarding aids in the visibility needed to determine IT-managed devices from BYOD. All this is necessary today.

Not only does this context help to better define policies, many organizations find it useful for solving wireless issues. Exceeding an expected device count by 30% to 40% does not help network performance. Knowing how many devices are 802.11ac versus 802.11n Wi-Fi enabled and which operating systems (iOS versus Android) users are carrying is also extremely valuable.

Extended Enterprise Visibility

As the volume of authentications and collected data increases, legacy AAA solutions lack the horsepower to keep up. Next-gen policy solutions built for mobility deliver the performance and coverage needed. It's not surprising to see over 100,000 authentications per day on a smaller campus where users roam between buildings.

While ClearPass can archive data, most organizations are now taking advantage of Security Information and Management (SIEM) to correlate data from multiple solutions – most of the same vendors that participate in the overall Adaptive Trust model and ClearPass Exchange program.

The greater visibility and a SIEMs ability to leverage advanced analytics for threat and risk mitigation make it great for keeping users and devices from behaving poorly and doing large scale damage.

SECTION 4:
Building a Trusted Defense

Industry Projections

When looking at the number of smart phones expected in the near future, the number ranges from 2 to 2.6 billion. This number does not account for tablets. The potential issues grow exponentially when these devices make their way onto your enterprise and guest networks.

While wired networks require similar security measures due to cabling issues, Gartner predicts that by 2018, 40% of enterprises will specify Wi-Fi as their default connection. They also predict that by 2020, more than 25 billion devices will be connected to the Internet compared to the five billion devices that are connected today.

The changes stem from the adoption of Internet of Things (IoT) in the consumer and enterprise space. IoT devices can range from smart meters and IV pumps, to HVAC systems used in office, healthcare, and retails spaces.

IDC predicts that by 2018, 50% of IT networks will transition from having excess capacity to being at capacity due to IoT. Policy management, profiling and enforcement to accurately delineate traffic type by device type will also play a role in network performance and security.

The choice is yours.

Next Steps – Planning for the Future

The choice is yours. Wait for users to circumvent static policies or create an environment that securely fosters collaboration and productivity, regardless of user role, device or location.

If you've made it this far, you've clearly decided to take a leadership role to assess how and where policy enforcement, device management, applications traffic inspection and visibility can take your business.

a Hewlett Packard
Enterprise company

For more info, visit
www.arubanetworks.com/clearpass