WHITE PAPER

THE ARUBA ADAPTIVE TRUST™ DEFENSE FOR SECURE ENTERPRISE MOBILITY

LEVERAGING REAL-TIME CONTEXT TO MITIGATE TODAY'S NEW RISKS

aruba NETWORKS an HP company

TABLE OF CONTENTS

THE NEW ENTERPRISE PERIMETER

There is a tectonic shift underway in today's enterprise networks. They're moving away from fixed, static wired networks to an open, dynamic environment where mobility rules and users – known as #GenMobile – enjoy anywhere, anytime access to enterprise resources.

#GenMobile, armed with a growing number of personal devices and apps, is taxing IT and security administrators by demanding greater access to company resources via Wi-Fi and cellular.

As BYOD initiatives continue to gain momentum, many enterprises are slow to respond due to a lack of policy management. At the same time, network security investments remain focused on shoring-up perimeter defenses, which fail to consider the challenges of mobility.

As a result, enterprises are struggling to secure data and mitigate new risks associated with mobility. Gateway firewalls, IDS/IPS, AV, anti-spam, URL filtering and other perimeter security solutions work well against external attacks. But many serious threats now originate from within the enterprise.

Mobility challenges the notion of a fixed perimeter and traditional defense mechanisms. Smart devices walk right through the front door, bypassing security controls and connecting directly to the network without IT's knowledge. In a mobile world, the network perimeter is anywhere and everywhere users connect, impairing the effectiveness of gateway defenses.

THE MOBILE RISK SPECTRUM

Today's sophisticated and persistent attacks target the lowest common denominator and gain a foothold through any exposed weakness or unguarded backdoor. A lack of policy control and limited visibility into mobile devices leaves enterprises vulnerable to a variety of new risks.

Threats associated with mobile devices are different. The ability to use these devices anywhere and store sensitive data on them dramatically increases the potential for data loss.

Additionally, their portability and small size makes them easily lost or stolen, often without password protections enabled. In fact, data loss due through misplaced devices is often cited as the top concern for IT administrators in charge of mobile security.

Beyond data loss, there are a variety of other variables that must also be considered when attempting to plug the security gaps introduced by mobility. These include:

- **User habits and behavior** – Mobile users have a nasty habit of bypassing IT controls to bring their own technology into the workplace. They use unauthorized apps and cloud storage – sometimes unwittingly – and access sensitive enterprise data outside of corporate controls in the name of improved productivity.
- **Loss of data controls** – Managing data in the mobile enterprise is complicated. Corporate enterprise data now extends beyond containers and apps to include offsite backup devices, unauthorized cloud systems and outsourced service providers utilized by employees.
- **Device churn** – New devices with different security controls are constantly replaced, which keeps IT guessing on what is actually on the network and how deal with them. Unauthorized changes or jailbroken device operating systems open the door to additional vulnerabilities.
- **Always-on, always-connected** – Sensitive data is now more easily exposed to untrusted, open, rogue and ad hoc networks as well as man-in-the-middle attacks as mobile devices seek out any available Wi-Fi network.

Traditional security measures that protected fixed endpoints and well-defined data paths are woefully inadequate for securing today's mobile enterprise. Security controls should adapt to the dynamic nature of users connecting and threats originating from anywhere.

What's more, the trust models established for employees who use corporate-issued devices no longer applies in a BYOD world. Trust is not something that can be assumed any longer; trust must now be earned and tracked to determine appropriate access rights and privileges.

A user who provides the appropriate credentials should not necessarily have carte blanche access. User names and passwords are insufficient in granting access rights to resources, especially if a user location and device are not under enterprise domain control.

Relevant contextual information – user role, device type, ownership and location – is missing from the traditional model. It allows IT to adapt policies that allow or deny access on a case by case basis without leaving enterprises exposed and exploitable to new threats.

Organizations need a new approach to secure mobile enterprise networks. One that leverages and shares context, applies adaptive controls based on mobility needs, and does so without hampering employee productivity.

INTRODUCING THE ARUBA ADAPTIVE TRUST™ DEFENSE

Security is often seen as a barrier to employee productivity. Cumbersome processes and strict policies tend to be bypassed, exposing enterprises to further exploits and a greater loss of control.

While they struggle with the risks introduced by enterprise mobility, employees continue to demand access for even more devices. Network and security teams must be aligned to ensure that essential services are available while appropriate security policies are followed.

Point-product solutions that address specific security needs can mitigate risks but lead to added complexity and limited controls. Loose integration between solutions also makes it difficult for IT to identify and react to the changing needs of a mobile workforce.

Aruba Adaptive Trust shares rich contextual data across disparate network security solutions to eliminate any potential security gaps. The result is a coordinated defense where all security components function as one integrated system without affecting employee productivity.

With this defensive framework, enterprise access management systems can easily leverage context from a multitude of sources to scrutinize user and device status before and after they connect.

Even better, this data is exchanged with enterprise mobility management (EMM), network firewalls, intrusion prevention systems, and other security solutions. The glue that makes it all work consists of common representational state transfer (REST) APIs and syslog-type data feeds.

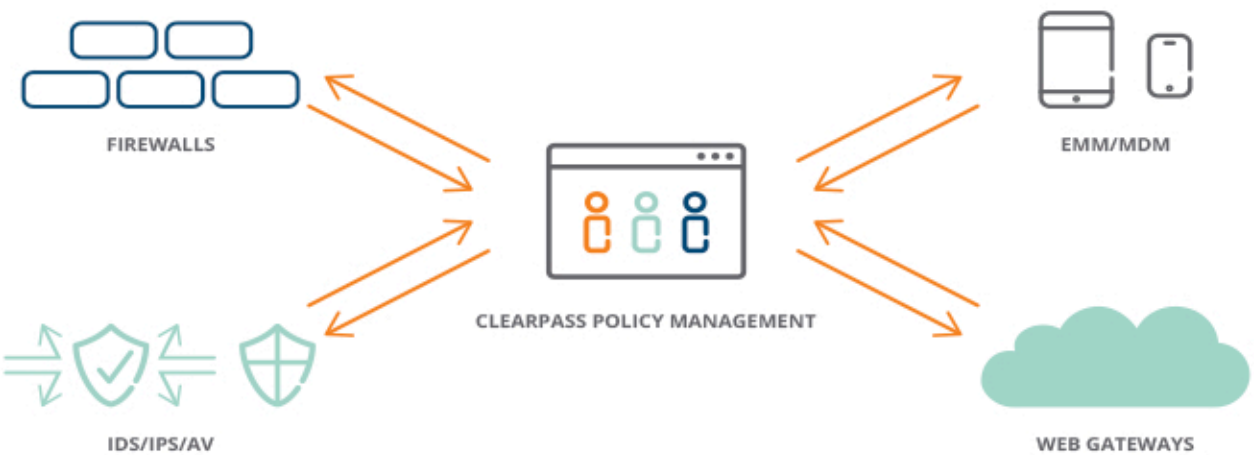
ARUBA ADAPTIVE TRUST ADDRESSES TODAY'S ACCESS SECURITY CHALLENGES

- **Context-based decisions** – Real-time contextual data ensures that security measures are enforced, regardless of user, device type or location. Policies are centrally managed and enforced when connecting via Wi-Fi, wired or VPNs.
- **Device compliance** – All devices must meet security and posture guidelines before connecting to the network. Devices that are not in compliance are required to remediate or are denied access.
- **Secure workflows** – Only authorized users can initiate a workflow based on IT policies. Personal devices must be allowed by policies to connect to enterprise resources. Backdoors are closed before they can be exploited.

This removes the complex scripting languages and tedious manual configuration needed for existing security solutions to work together more effectively to combat the risks associated with enterprise mobility.

Aruba Adaptive Trust lets IT make smarter decisions about how users and devices connect and how their access privileges are enforced. Consequently, a centralized policy enforcement engine becomes the central nervous system for all things connecting to the network.

ADAPTIVE TRUST DEFENSE



Aruba ClearPass leverages and shares contextual data about users, devices and locations with a variety of network tools for more granular policy definition and enforcement.

figure 1.0_010915_adaptivetrust-wpa