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

THE ARUBA DIFFERENCE

The ClearPass Access Management System provides the foundation for the Aruba Adaptive Trust defense model. It provides central control and mobile security enforcement based on roles, and real-time contextual information on any multivendor network.

This unique approach, based on the ClearPass Exchange common-language integration, enables enterprise organizations to leverage contextual information across security systems for granular and accurate policy enforcement.

ClearPass delivers secure enterprise mobility by integrating policy management with AAA, guest network access, secure onboarding, device health checks, and other self-service capabilities – all from one platform.

ClearPass also enables two-factor authentication by leveraging multiple identity stores within one service, including Microsoft Active Directory, LDAP-compliant directories, ODBC-compliant SQL databases, token servers and internal databases.

Providing an invaluable source of additional context, identity stores can also be utilized to authenticate users and authorize the use of specific enterprise resources.

ClearPass Exchange support for REST APIs and data feeds allows crucial enterprise mobility intelligence to be shared between ClearPass and other security solutions and business workflow systems.

Consequently, Palo Alto® Networks Next-Generation Firewalls can automatically leverage user and device context for granular app-level policies. And EMM applications like MobileIron are now able to share user, device and location visibility for security Wi-Fi enforcement.

CLEARPASS OFFERS A WIDE RANGE OF FEATURES THAT ENABLE SECURE ENTERPRISE MOBILITY

- **Enhanced visibility** – dynamic profiling of devices as they connect provides valuable information that can be used within policies and for troubleshooting.
- **Enterprise-ready policies** – built-in policy service templates deliver where legacy AAA solutions fail. BYOD initiatives and guest access services are created and usable with minutes.
- **Centralized context** – all collected data like location, device type and status, and device ownership is usable and shared with existing security solutions from a central repository.
- **Self-service** – users are allowed to self-configure personal devices, revoke certificates for lost devices and sponsor guest access, which reduces IT helpdesk tickets while increasing productivity for all.
- **Enforcement built for mobility** – managing separate VLANs to enforce network privileges based on traffic types is complex and burdensome. Policies for mobile devices requires leveraging roles, traffic types and other contextual data to automatically direct users to appropriate network segments. VLAN and ACL enforcement is only used when required.

Interaction with helpdesk tools like ServiceNow® automatically initiates a helpdesk ticket with vital information about the user, device and access problem in the event of a network authentication failure.

DATA EXCHANGED WITH OTHER NETWORK TOOLS

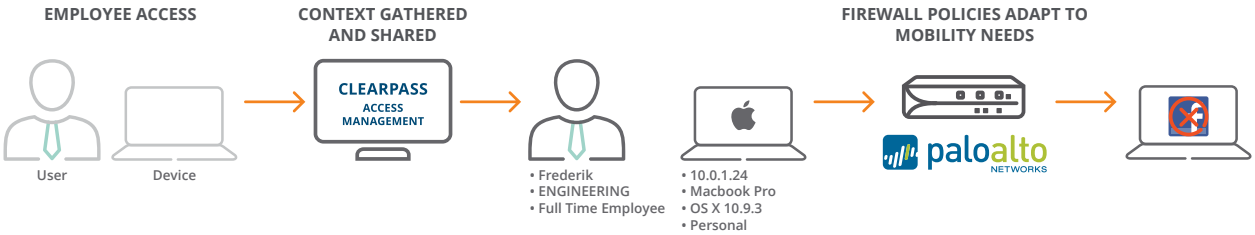


figure 2.0_011915_adaptivetrust-wpa

USING ARUBA ADAPTIVE TRUST FOR SECURE ENTERPRISE MOBILITY

ClearPass addresses the needs of the ever-changing policy landscape and replaces point solutions and management headaches with one comprehensive, secure, robust policy management system. This lowers capex and opex while opening a path to create finely-tuned security policies with an emphasis on simplicity and a better user experience for #GenMobile.

By leveraging context from multiple identity stores and authentication methods, ClearPass allows IT to create more granular enforcement policies. This means that corporate-managed and personal devices are treated differently on the same infrastructure.

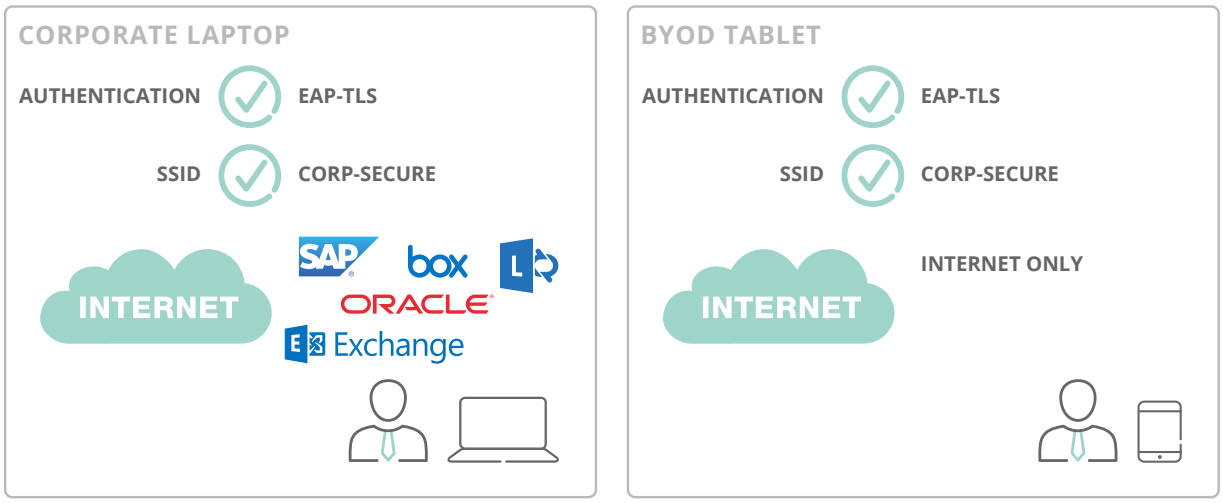
The result is a dynamic, integrated and robust solution that easily adapts network and security functions to the mobile needs of employees, allowing enterprise organizations to quickly tackle a wide range of common challenges.

BYOD AND IT-ISSUED DEVICES ON THE SAME SSID

Instead of broadcasting multiple SSIDs or creating complex VLAN mappings to accommodate BYOD, role-based enforcement and contextual policies let ClearPass easily differentiate access for personally-owned devices.

ClearPass also distributes and provisions device-specific credentials on each BYOD endpoint to limit or revoke access privileges. This dramatically simplifies the access infrastructure while improving security and lowering the provisioning burden on IT.

BYO AND CORPORATE DEVICES ON SAME SSID



ClearPass allows differentiated access on the same SSID based user, device and location information.

figure 3.0_011915_adaptivetrust-wpa

EXTEND IT CONTROLS TO DEVICES AT HOME

Ensuring that personal mobile devices conform to policies is no easy task, especially when they aren't physically connected to the network. ClearPass easily extends policy controls and enforcement to devices that connect from remote locations like home offices.

Persistent and dissolvable agents that are used with computers can likewise be utilized to ensure that all devices are thoroughly assessed and pass health checks before they access the enterprise network.

ClearPass also works with EMM systems, pulling contextual data from smartphones and tablets to trigger enforcement actions for any device requesting enterprise wired, wireless or VPN access. Context can include jailbroken status, white and black-listed apps, device type and more.

PREVENT BYOD ON GUEST NETWORKS

Guest networks allow guests and other VIPs to enjoy Wi-Fi connectivity during their visit, but are often misused by employees who attempt to bypass corporate BYOD policies for a network connection.

ClearPass can quickly determine if a BYOD or IT-managed device belongs on the guest network by leveraging context gathered during device registration and onboarding. This limits the amount of enterprise data that is exposed on open guest networks.

AUTHORIZATION AND ENCRYPTION ON OPEN NETWORKS

Wi-Fi hotspots are a convenient means for remote employees and professionals who travel to stay connected to enterprise resources. Unfortunately, many of these hotspots are vulnerable to a variety of cyber threats and man-in-the-middle attacks.

To eliminate liabilities and safeguard customers, ClearPass offers an easy way to add enterprise-grade security on any public Wi-Fi network. Augmenting the protected extensible authentication protocol (PEAP) framework, ClearPass ensures that each guest sessions is encrypted and thus invisible to anyone trying to sniff Wi-Fi packets.

SUMMARY

Evolving user habits, threats, and mobile devices require a new approach to secure enterprise networks. The #GenMobile way of working has completely diluted the notion of a fixed perimeter – it doesn't exist in a mobile world where users connect and work from anywhere.

To that end, best-of-breed policy management, NAC, network firewall, and EMM systems must find a common way to share and protect enterprise resources. It's time for centrally-managed policies, secure BYOD and guest access workflows that enable IT to deliver secure enterprise-class mobility that minimizes risks.

ClearPass is the heart of the Aruba Adaptive Trust model. It acts as a centralized gatekeeper and contextual store for all user authentication and device data. ClearPass identifies and authenticates users and devices, trust-based rules grant appropriate access privileges based on specific needs.

By employing the Aruba Adaptive Trust model, enterprise IT organizations can ensure that the growing risks associated with mobility are addressed at the point of authentication and beyond, with a higher degree of user and IT satisfaction.

ABOUT ARUBA NETWORKS, AN HP COMPANY

Aruba Networks, an HP company, is a leading provider of next-generation network access solutions for the mobile enterprise. The company designs and delivers Mobility-Defined Networks that empower IT departments and #GenMobile, a new generation of tech-savvy users who rely on their mobile devices for every aspect of work and personal communication. To create a mobility experience that #GenMobile and IT can rely upon, Aruba Mobility-Defined Networks™ automate infrastructure-wide performance optimization and trigger security actions that used to require manual IT intervention. The results are dramatically improved productivity and lower operational costs.

To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Social at http://community.arubanetworks.com.

aruba NETWORKS an HP company

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