aruba
a Hewlett Packard Enterprise company

PARTNER SOLUTION OVERVIEW

ARUBA & IBM SECURITY

Redefining Authentication and Authorization with Aruba ClearPass

IBM Security and Aruba Networks unify network access policy, mobile device management (MDM) and application accessibility for security and convenience.

Managing user authentication and single sign-on for web application can be increasingly challenging as endpoints are used to secure enterprise applications. IBM Security Access Manager and Aruba ClearPass provide a powerful way to extend risk-based access control across multiple application types for consistent security policies. Together, this joint solution unifies network access policy, mobile device management (MDM), and application accessibility for security and convenience.

Customers can now use real-time network authentication attributes to securely provide access to protected applications across wireless, wired, and VPN environments.

OVERCOMING APPLICATION ACCESSIBILITY CHALLENGES

The popularity of bring-your-own-device (BYOD) initiatives has challenged IT to provide granular policies for securing access to cloud and mobile applications.

Users today may carry up to three endpoints, which limit the use of generic policies based on static attributes. IT now needs the ability to create context-aware policies that include the status of a user's network authentication as well as risk-based device assessments leveraged from MDM solutions like IBM's Fiberlink MaaS360.

The ideal scenario also ensures a correlation between a user, each device they connect to the network and per session network authentication credentials.

Subsequent access to protected web applications is then granted and differentiated based on device type, risk score and location. Logins to defined web applications will result in no additional username/password challenges.

WHY ARUBA AND IBM

- Extends IBM capabilities to include network authentication and device status
- Supports any existing multivendor network and endpoint environment
- Network authentication for Auto Sign-On to protected web applications
- Simplifies traditional user single sign-on limitations

THE IBM SECURITY AND ARUBA SOLUTION

The ability to provide users with the convenience of an Auto Sign-on to protected web resources using a seamless network logon requires the following components:

- IBM Security Access Manager for Web with ClearPass ISAM plugin (v7.0 or later)
- Aruba ClearPass Access Management System™ (v6.3 or later)
- Aruba Mobility Controller (ArubaOS v6.4 or later)

Optional components can include:

- IBM Security Access Manager for Mobile (v8.0 or later)
- Mobile Device Management – IBM/FiberLink Maas360, MobileIron, AirWatch, Citrix Xenprise or others

IBM® Security Access Manager (ISAM) for Web – safeguards access to web applications using contextaware access controls with added protection against advanced web threats.

IBM® Security Access Manager for Mobile – mobile access security protection enforces contextaware authorization through mobile device finger printing, geographic location awareness, and IP reputation for adaptive, risk-based access.

Aruba ClearPass Access Management System – a single multivendor platform for managing and enforcing role-based access policies for wireless, wired and VPN networks. Provides an external authentication interface for the ISAM suite that grants access based on network authentication and authorization data for Auto Sign-On to web applications.

Aruba Mobility Controller – hardened wireless controller that manages system operation functions using an embedded real-time operating system with dedicated packet-processing hardware for all routing, switching and firewall functions. Maintains network authorization state for access to web applications for Auto Sign-On functionality.

CERTIFIED INTEROPERABILITY

We've taken the guesswork out of device authentication and authorization by certifying the interoperability of MobileIron with Aruba ClearPass. Set-up is a breeze. When a user accesses the network and is re-directed to ClearPass for authentication, user-based policies are enforced and the user must request access to ISAM web/mobile resources. ISAM uses the data within ClearPass to assess and approve the request, creating a successful authentication when the identity of the user and device is confirmed. Auto sign-on is enabled for subsequent log-in attempts.

SUMMARY

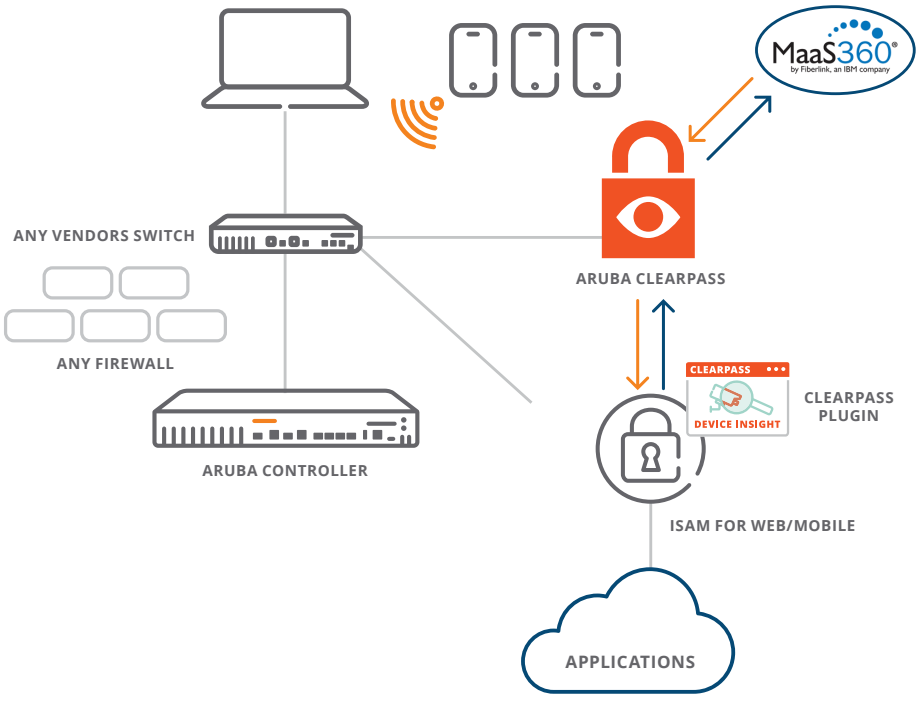
Together, IBM® Security Access Manager for Web and Mobile and Aruba's ClearPass platform provide a risk based access control system for protected web resources and a powerful multivendor policy engine and authentication platform.

Customer value extends beyond network infrastructure interoperability and enhanced security to a new level of user convenience.

To learn more about Aruba ClearPass, please visit: https://www.arubanetworks.com/products/security/network-access-control/

To learn more about IBM Security, please visit: https://www.ibm.com/security

Secure authentication and authorization workflow



a Hewlett Packard Enterprise company

PSO_IBMSecurity_081319 a00080321enw