aruba
a Hewlett Packard Enterprise company | mobileiron

PARTNER SOLUTION OVERVIEW

ARUBA & MOBILEIRON

A Better Way to Manage Smart Devices for Secure Enterprise Mobility

In today's mobility-centric workplace – smartphones and tablets are carried by everyone – including employees and contractors. Because of this, it's inevitable that they will contain a combination of personal and enterprise data. Infrastructure-wide policies are a best practice today that help automate how mobile devices are configured, remotely managed and used on enterprise networks.

It is important to ensure that if smartphones and tablets are replaced, lost, or stolen it is easy for IT to wipe them of critical enterprise data. Today, a lost or stolen device can mean a long day for the user and IT team, which presents a significant IT security risk and a much longer attacker dwell time. An automated management and policy management system is the key for faster resolution and peace of mind.

Aruba and MobileIron have partnered to integrate Aruba ClearPass Policy Manager and MobileIron's Unified Endpoint Management to simplify onboarding IT-managed and BYOD devices onto a network, with policy automation and enforcement that protects your enterprise data and network resources. Policies extend across cellular and Wi-Fi networks ensure that corporate applications and data are protected, regardless of device type or where it is being used.

INDUSTRY LEADING NETWORK ACCESS ENFORCEMENT

Aruba ClearPass provides enterprise network access control for automated device onboarding, device profiling, and policy enforcement. Together with MobileIron, Aruba ClearPass Policy Manager leverages user's roles, device types, location, and other attributes – in addition to status pulled from MobileIron managed devices to properly set access privileges for wireless, wired and VPN access.

WHY ARUBA & MOBILEIRON?

- Simple to use detection of compromised devices, denylisted applications, and other policy violations on the endpoint
- Flexible policy creation that enables near real-time monitoring of device security posture and policy compliance for network access control and dynamic segmentation of devices on the network
- Real-time endpoint event logs for faster time to resolution of issues, and containment of compromised or otherwise non-compliant devices
- Certified joint interoperability

ClearPass first syncs NAC profile data by retrieving device details for all the mobile endpoints and then retrieves the device data and events notifications to give it a near real-time context update for the endpoints. This ensures that the latest status of the device is being used to make access control decisions upon initial connection to the network, and also to quarantine or limit access by that device to the network if the status of that device changes.

Use Cases:

- Monitor for device registration events
- Monitor for compliance events
- Monitor for Device Tagged "compliant" "non-compliant"
- Periodic full rebase or scan of device objects and attributes
- Force a device check in by UEM identifier
- Privacy policy and selective wipe for secure corporate data and personal data protection

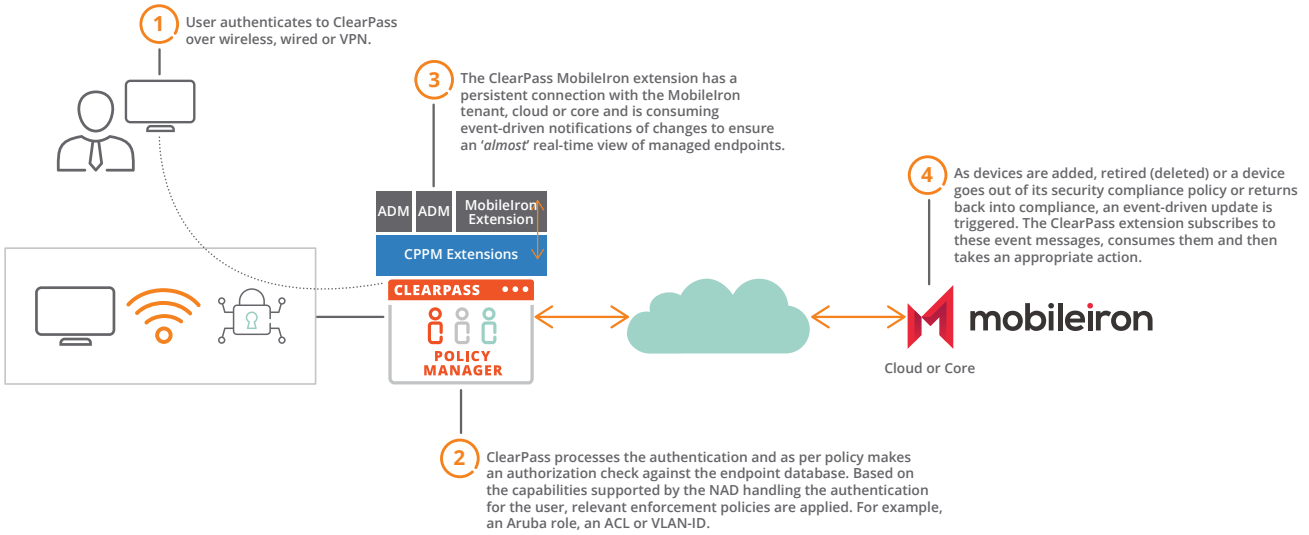

Figure 1: Aruba and MobileIron joint solution diagram

FEATURES AND BENEFITS

Jailbreak Status

A common use case is to leverage the presence of the UEM agent to detect if a device has been jailbroken (Apple iOS) or had a root-kit installed (Android). ClearPass allows IT to automatically enforce access rules for any compromised devices when these conditions are met as they are connecting to the network. Granted access can be limited to minimize risk, or completely denied if policies are not met.

Denylisted Apps

To strengthen compliance policies, denylisted apps can be defined and checked via MobileIron. ClearPass then polls the MobileIron solution to detect if denylisted apps are being used and redirects users to a remediation portal, where the policy breach is explained, and remediation instructions can be provided. Optionally, network access can be restricted until the device is remediated.

The Removal of the Mobileiron Agent

Whether deliberately or accidentally, if the removal of an UEM agent or profile from a device prevents MobileIron from enforcing policies, ClearPass can use this context and redirect the user to a portal to re-install the agent before granting network access.

The above examples represent only a small number of possible scenarios in which IT organizations can utilize UEM and network access security to ensure that mobile device policies are enforced across cellular and wireless networks.

Enhanced Integration Capabilities

Using two-way interaction, MobileIron leverages network events to prompt ClearPass Exchange to perform any required action, such as quarantining or wiping the device. If a policy is violated, a notification can automatically be sent to the user explaining why the device action was taken.

When using certificates for authentication, ClearPass can act as a certificate authority to ensure that each device contains a unique certificate. The value of utilizing the ClearPass certificate is that device information and user data is built into the certificate. This adds value by including more than data about the organization for which the certificate was issued, providing additional levels of trust for the device.

Real Time Framework

In order to react to cyber and threat driven events, the ClearPass Policy Manager can ingest and process externally generated alerts in multiple formats including REST API, webhook, syslog, and more. Historically, NAC vendors would integrate with UEM vendors to ingest endpoint data based upon a polling process which would provide a view of all managed endpoint data, which would not provide up to date status of the device, possibly resulting in compromised or infected devices connecting to your network. With the ClearPass Policy Manager real time framework, ClearPass receives these critical events in near real-time, enabling additional levels of trust in the device that's connecting to your network.

Together, MobileIron and Aruba can generate real time event updates where ClearPass Policy Manager is aware of new or deleted endpoints, or devices where compliance has changed. All of this happens in around 3 to 5 seconds.

SUMMARY

Together, Aruba and MobileIron provide organizations with policy management that does it all – a complete solution for mobile device and network access security, with optimized policies and complete authentication, authorization and accounting (AAA) services for any BYOD or IT-managed deployment. IT organizations can now better secure their networks using utilize real-time employee data, device attributes and their status, application use, and location.

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

To learn more about MobileIron, please visit: https://www.mobileiron.com/en

PSO_MobileIron_102020 a00081784enw