aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

AIRWATCH® AND ARUBA CLEARPASS FOR ENTERPRISE MOBILITY

SECURE MOBILITY FOR MOBILE DEVICES ON ANY NETWORK

Remember when BlackBerry devices ruled the mobile roost? Enterprises were comfortable with them, and so were users. They had secure end-to-end control, with critical feedback and control points at the device and network to protect enterprise data and network resources. This solved the end-user and IT dilemma for simple and secure access to email from anywhere.

But in today's mobile world, apps and devices have evolved well beyond email. Implementing Enterprise Mobility Management (EMM) to address secure corporate access for today's popular device operating systems and apps for secure enterprise mobility is key.

Luckily, AirWatch and Aruba ClearPass provide an end-to-end secure solution to fill the gap.

- EMM context sharing provides needed data for secure enterprise network decisions.
- Automated network access and business workflows before and after devices connect.
- Industry and innovation leadership per Gartner's Magic Quadrants.

AIRWATCH AND CLEARPASS WORKING TOGETHER

Network security is now more relevant for mobile devices

- For strong network policy enforcement, AirWatch shares contextual information about devices with ClearPass.
- Jailbreak/root-kit detection – Unhealthy devices detected by AirWatch are denied access or quarantined by ClearPass.
- ClearPass posture assessments for missing EMM agents or denylisted apps can trigger appropriate access enforcement, remediation and notifications.

Easily tie mobile security enforcement to the rest of your business

- Create business-relevant network rules – location and denylisted apps can trigger relevant security actions on mobile devices and change network privileges accordingly.
- Invoke critical non-network device actions – ClearPass Exchange APIs let IT automate and improve common business workflows such as IT helpdesk ticketing and device notifications.

Streamlined certificate enrollment with integrated network policy enforcement

- Built-in ClearPass certificate authority eliminates login and passwords on mobile devices for improved security and user experience.

"Securing the Experience Edge"

FREQUENTLY ASKED QUESTIONS

Q: Why should I allow mobile devices to connect to Wi-Fi?

- Superior indoor coverage, speed and app security.
- Cost avoidance: Data overage and roaming charges.

Q: Why ClearPass for enterprise Wi-Fi connectivity?

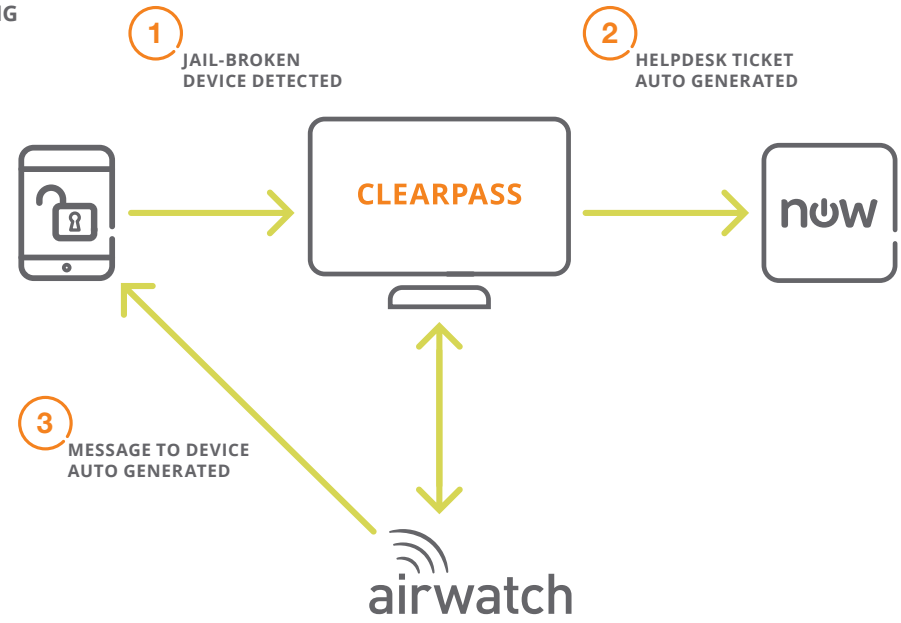
- Network access enforcement that builds on AirWatch's device and app policies.
- Policies based on user role, device and location attributes.

Q: How does AirWatch/ClearPass integration differ from competing solutions?

- A major difference lies in the ability to trigger customer-defined policies that broaden enforcement and notification capabilities. Other NAC solutions only enforce policies at the network layer.
- ClearPass offers a fully integrated certificate authority for 802.1X certificate provisioning, management and revocation.

END-TO-END ACCESS AND NOTIFICATION WORKFLOW WITH AIRWATCH

JAILBREAK DETECTION WORKFLOW TRIGGERING AUTOMATIC HELPDESK WORKFLOW THROUGH SERVICENOW AND USER NOTIFICATION THROUGH AIRWATCH



aruba
a Hewlett Packard Enterprise company

SO_AirWatch_101420